

10/500152

(特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004年6月24日 (24.06.2004)

PCT

(10) 国際公開番号
WO 2004/053699 A2

(51) 国際特許分類7: G06F 12/14, H04L 9/08, G11B 20/10

(21) 国際出願番号: PCT/JP2003/015525

(22) 国際出願日: 2003年12月4日 (04.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-355114 2002年12月6日 (06.12.2002) JP

(71) 出願人(米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 木谷聰 (KITANI,Satoshi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 杉浦正知, 外 (SUGIURA,Masatomo et al.); 〒171-0022 東京都豊島区南池袋2丁目49番7号 池袋パークビル7階 Tokyo (JP).

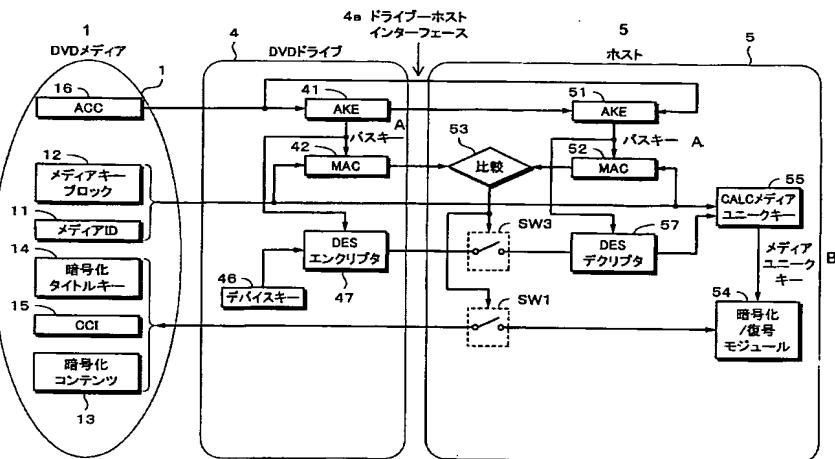
(81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[統葉有]

(54) Title: RECORDING/REPRODUCTION DEVICE, DATA PROCESSING DEVICE, AND RECORDING/REPRODUCTION SYSTEM

(54) 発明の名称: 記録再生装置、データ処理装置および記録再生処理システム



1...DVD MEDIUM
11...MEDIUM KEY BLOCK
11...MEDIUM ID
14...ENCRYPTION TITLE KEY
13...ENCRYPTION CONTENT
4a...DRIVE-HOST INTERFACE
4...DVD DRIVE
A...BUS KEY

46...DEVICE KEY
47...DES ENCRYPTER
5...HOST
53...COMPARISON
55...CALC MEDIUM UNIQUE KEY
57...DES DECRYPTER
B...MEDIUM UNIQUE KEY
54...ENCRYPTION/DECRYPTION MODULE

(57) Abstract: A device key (46) is mounted on a drive (4) side. In order to securely send the device key (46) to a host (5), the device key (46) is encrypted by a bus key. At the host (5) side, the device key is decrypted by the bus key. A medium unique key calculation block (55) calculates the medium unique key from an MKB (12), a medium ID, and a decrypted device key (46). In the calculation block (55), when the calculated medium key becomes

[統葉有]

WO 2004/053699 A2



TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書なし；報告書を受け取り次第公開される。

a predetermined value, the drive (4) is revoked and the processing is terminated. The medium unique key is supplied to an encryption/decryption module (54) and a content key is obtained from an encryption title key (14) and a CCI (15). By using the content key, the encrypted content is decrypted and the content to be recorded is encrypted.

(57) 要約: デバイスキ-4 6 がドライブ 4 側に実装される。デバイスキ-4 6 をセキュアにホスト 5 に伝送するために、デバイスキ-4 6 がバスキーで暗号化される。ホスト 5 側で、バスキーでデバイスキ-4 6 が復号される。メディアユニークキー演算ブロック 5 5 が MKB 1 2 とメディア ID と復号されたデバイスキ-4 6 とからメディアユニークキーを演算する。演算ブロック 5 5 において、計算されたメディアキーが所定の値となる場合には、ドライブ 4 がリボーカされ、処理が停止される。メディアユニークキーが暗号化/復号モジュール 5 4 に供給され、暗号化タイトルキー 1 4、CCI 1 5 からコンテンツキーが求められ、コンテンツキーを使用して暗号化コンテンツが復号され、記録されるコンテンツが暗号化される。

明細書

記録再生装置、データ処理装置および記録再生処理システム

技術分野

5 この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される記録再生装置、データ処理装置および記録再生処理システムに関する。

10 背景技術

近年開発されたD V D (Digital Versatile Disc)等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して

15 著作権の保護を図ることがますます重要となっている。

D V D - Video では、コピー・プロテクション技術としてC S S (Content Scrambling System) が採用されている。C S S は、D V D メディアに対する適用のみが認可されており、D V D - R、D V D - R W 、D V D + R、D V D + R W 等の記録型D V D でのC S S の利用がC 20 S S 契約によって禁止されている。したがって、D V D - Video の内容を記録型D V D へのまるごとコピー（ビットバイビットコピー）は、C S S 契約上では、認められた行為ではない。

しかしながら、C S S の暗号方式が破られる事態が発生した。C S S の暗号化を解除してD V D - Video の内容を簡単にハードディスク 25 にコピーする「D e C S S」と呼ばれる違法なソフトウェアがインターネット上で配布された。「D e C S S」が出現した背景には、本来

耐タンパー化が義務付けられているはずのCSS復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にCSSアルゴリズム全体が解読された経緯がある。

5 CSSの後に、DVD-Audio等のDVD-ROMの著作権保護技術であるCPPM(Content Protection for Pre-Recorded Media)、並びに記録型DVD、メモリカードに関する著作権保護技術CRPM(Content Protection for Recordable Media)が提案されている。これらの方程式は、コンテンツの暗号化や管理情報の格納等に問題が生じ
10 たときに、システムを更新でき、データをまるごとコピーしても再生を制限できる特徴を有している。DVDに関する著作権保護の方法に関しては、下記の非特許文献1に説明され、CRPMは、ライセンス管理者である米4C Entity, LLCが配布する下記の資料に説明されている。

15 山田、「DVDを起点に著作権保護空間を広げる」、日経エレクトロニクス 2001.8.13, p.143-153
"Content Protection for Recordable Media Specification DVD Book"、インターネット<URL : <http://www.4Centity.com/>>
20 パーソナルコンピュータ（以下、適宜PCと略す）環境下では、PCとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

著作権保護技術をPC上で実行されるアプリケーションプログラム

へ実装する際には、その著作権保護技術の解析を防ぐため耐タンパ
性を持たせるのが一般的である。しかしながら、耐タンパ性の強度
を示す指標がない。その結果、どの程度のリバースエンジニアリング
への対応を行うかは、インプレメンターの個々の判断や能力に委ねら
れていのが現状である。CSSの場合は、結果として破られてしま
った。CSSの後に提案されたCPPMおよび記録型DVDに関する
著作権保護技術CRPMにおいても、PCでのソフトウェア実装に関する
問題解決に至る技術的方法の提案がなされていない。

この発明の目的は、PC環境下でも著作権保護技術の安全性を確保
することである。すなわち、正規のライセンスを受けないドライブの
作成を防止し、さらに、確実にリボケーションを行うことが可能な記
録再生装置、データ処理装置および記録再生処理システムを提供する
ことにある。

15 発明の開示

上述した課題を解決するために、この発明の第1の態様は、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

20 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

記録媒体固有の第1の情報と格納部に格納された第2の情報に基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

を有する記録再生装置である。

この発明の第2の態様は、少なくとも格納部に格納された第2の情報と記録媒体固有の第1の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリポケーションを行うリボーカー処理部を有するデータ処理装置に対して、接続部が格納部に格納された第2の情報を送る記録再生装置である。

この発明の第3の態様は、格納部に格納された第2の情報と記録媒体固有の第1の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリポケーションを行うリボーカー処理部を有する記録再生装置である。

この発明の第4の態様は、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェア固有にのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

記録媒体固有の第1の情報と格納部に格納された第2の情報に基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

少なくとも接続部を介してデータ処理装置から送られ、格納部に格納された第2の情報と、記録媒体固有の第1の情報を用いて、当該格納された第2の情報が正当なアプリケーションソフトウェア固有の

情報でない場合にリボケーションを行うリポーク処理部を有する記録再生装置である。

この発明の第 5 の態様は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーション 5 ソフトウェア固有の第 2 の情報を有するとともに、記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

接続部を介して記録再生装置から送られた、記録媒体固有の第 1 の 10 情報と電子機器またはアプリケーションソフトウェア固有の第 2 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部と 15 を有するデータ処理装置である。

この発明の第 6 の態様は、接続部を介して記録再生装置から送られ 15 た第 2 の情報と、記録媒体固有の第 1 の情報を用いて、第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリポーク処理部を有するデータ処理装置である。

この発明の第 7 の態様は、少なくとも記録再生装置に格納された第 20 2 の情報と、記録媒体固有の第 1 の情報を用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリポーク処理部を有する記録再生装置と接続するデータ処理装置である。

この発明の第 8 の態様は、正当なアプリケーションソフトウェアに 25 のみ与えられるアプリケーションソフトウェア固有の第 2 の情報を有する格納部と、

記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

5 記録媒体固有の第 1 の情報と格納部に格納された第 2 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部とを有し、

格納部に格納された第 2 の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を
10 有する記録再生装置に対して、格納部に格納された第 2 の情報を送るデータ処理装置である。

この発明の第 9 の態様は、記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方が可能であると共に
15 正当な電子機器またはアプリケーションソフトウェア固有にのみ与えられる電子機器またはアプリケーションソフトウェア固有の第 2 の情報を有する記録再生装置と、

少なくとも格納された第 2 の情報と、記録媒体固有の第 1 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と
20 を有する記録再生処理システムである。

この発明の第 10 の態様は、データ処理装置が記録媒体固有の第 1 の情報と格納された第 2 の情報を用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報で
25 ない場合にリボケーションを行うリボーク処理部を有する記録再生処理システムである。

この発明の第 1 1 の態様は、記録再生装置が記録媒体固有の第 1 の情報と格納された第 2 の情報を用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリポケーションを行うリボーカー処理部を有する記録再生処理

5 システムである。

この発明の第 1 2 の態様は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報として格納された第 2 の情報を有するとともに、記録媒体固有の第 1 の情報を保持している記録媒体への暗号化

10 されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と、

格納された第 2 の情報と、記録媒体固有の第 1 の情報とに基づいて生成された鍵を用いてデータの暗号化、または暗号化されたデータの復号が可能なデータ処理装置とからなり、

15 格納された第 2 の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリポケーションを行うリボーカー処理部を有する記録再生装置に対して、データ処理装置が格納部に格納された第 2 の情報を送る記録再生処理システムである。

この発明の第 1 3 の態様は、不正な電子機器を無効化するための第

20 1 の情報と、コンテンツ毎に異なる第 2 の情報と、暗号化単位毎に定義可能な第 3 の情報と、スタンバ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

25 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 4 の

情報が格納される格納部と、

上記第1の情報と上記第4の情報とから当該格納された第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であるかを判定するリボーグ処理部と、

- 5 上記リボーグ処理部で上記第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、上記第1の情報、上記第4の情報、上記第2の情報および上記識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と有する記録再生装置である。
- 10 この発明では、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報例えばデバイスキーが記録再生装置に格納されている。したがって、デバイスキーを外部から読み取ることが不可能となり、データ処理装置にインストールされるアプリケーションは、著作権
- 15 保護技術に関するデータを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。また、記録媒体を扱う正当な記録再生装置となるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規の
- 20 ライセンスを受けずに正規品になりますのようなクローン装置の作成を防止できる効果がある。

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。その結果、データ処理装置にインストールされるアプリケーションは、

- 25 著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に

対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

図面の簡単な説明

5 第1図は、先に提案されているレコーダ、プレーヤおよびDVDメディアからなるシステムを説明するためのブロック図である。

第2図は、PCベースのDVDメディア記録再生システムを説明するためのブロック図である。

10 第3図は、第2図のシステムにおけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

第4図は、第2図のシステムにおける認証動作を説明するためのフローチャートである。

第5図は、この発明の第1の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

15 第6図は、この発明の第1の実施形態におけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

第7図は、この発明の第2の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

20 第8図は、この発明の第3の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

第9図は、この発明の第3の実施形態におけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

第10図は、この発明の第4の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

25 第11図は、この発明の第4の実施形態におけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

第12図は、この発明の第5の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

第13図は、この発明の第6の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

5 第14図は、この発明の第6の実施形態におけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

第15図は、この発明の第7の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

10 第16図は、この発明の第7の実施形態におけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

第17図は、この発明の第8の実施形態によるPCベースの書き込み可能なメディアの記録再生システムのブロック図である。

第18図は、この発明の第9の実施形態によるPCベースのROMタイプのメディアの再生システムのブロック図である。

15

発明を実施するための最良の形態

この発明の理解の容易のために、最初に第1図を参照して著作権保護技術例えばDVD用CPRMのアーキテクチャについて説明する。

第1図において、参照符号1が例えばCPRM規格に準拠したDVD-R/RW、DVD-RAM等の記録型DVDメディアを示す。参照符号2が例えばCPRM規格に準拠したレコーダを示す。参照符号3が例えばCPRM規格に準拠したプレーヤを示す。レコーダ2およびプレーヤ3は、機器またはアプリケーションソフトウェアである。

未記録ディスクの状態において、DVDメディア1の最内周側のリードインエリアのBCA(Burst Cutting Area)またはNBCA(Narrow Burst Cutting Area)と称されるエリアには、メディアID11が

記録されている。リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキープロック（以下、MKBと適宜略す）12が予め記録されている。メディアID11は、個々のメディア単位例えばディスク1枚毎に異なる番号であり、メディアの製造者コードと5シリアル番号から構成される。メディアID11は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキープロックMKBは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアIDおよびメディアキープロックは、記録媒体固有の第101の情報である。

ディスク1の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ13が記録される。暗号化方式としては、C2 (Cryptomeria Ciphering) が使用される。

DVDメディア1には、暗号化タイトルキー14およびCCI (Copy Control Information) 15が記録される。暗号化タイトルキー14は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。CCIは、コピー一モア、コピー一ワナス、コピーフリー等のコピー制御情報である。

レコーダ2は、デバイスキーエンボス21、プロセスMKB22、C2_G23、乱数発生器24、C2_E25、C2_G26およびC2_E27の構成要素を有する。プレーヤ3は、デバイスキーエンボス31、プロセスMKB32、C2_G33、C2_D35、C2_G36およびC2_DCB37の構成要素を有する。

デバイスキーエンボス21、31は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーエンボスは、ライセンス管理者によって正当な電子機器またはアプリケ

ーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。D V D メディア 1 から再生されたM K B 1 2 とデバイスキー 2 1 とがプロセスM K B 2 2 において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ 2 におけるのと同様に、プレーヤ 3 においても、M K B 1 2 とデバイスキー 3 1 とがプロセスM K B 3 2 において演算され、リボケーションされたかどうかの判別がなされる。

プロセスM K B 2 2 、 3 2 のそれぞれにおいて、M K B 1 2 とデバイスキー 2 1 、 3 1 からメディアキーが算出される。M K B 1 2 の中にレコーダ 2 またはプレーヤ 3 のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ 2 またはプレーヤ 3 が正当なものでないと判断される。すなわち、そのようなレコーダ 2 またはプレーヤ 3 がリボケーションされる。

C 2 _ G 2 3 、 3 3 は、それぞれ、メディアキーとメディア I D を演算し、メディアユニークキーを導出する処理である。

乱数発生器 (R N G : Random Number Generator) 2 4 は、タイトルキーの生成に利用される。乱数発生器 2 4 からのタイトルキーがC 2 _ E 2 5 に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー 1 4 がD V D メディア 1 に記録される。

プレーヤ 3 では、D V D メディア 1 から再生された暗号化タイトルキー 1 4 とメディアユニークキーとがC 2 _ D 3 5 に供給され、暗号化タイトルキーがメディアユニークキーで復号化され、タイトルキーが得られる。

レコーダ 2 においては、C C I とタイトルキーとがC 2 _ G 2 6 に供給され、コンテンツキーが導出される。コンテンツキーがC 2 _ E

CBC27に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ13がDVDメディア1に記録される。

プレーヤ3においては、CCIとタイトルキーとがC2_G36に供給され、コンテンツキーが導出される。コンテンツキーがC2_D

5 C BC37に供給され、DVDメディア1から再生された暗号化コンテンツ13がコンテンツキーを鍵として復号される。

第1図の構成において、レコーダ2による記録の手順について説明する。レコーダ2は、DVDメディア1からMKB12を読み出し、プロセスMKB22によってデバイスキー21とMKB12とを演算

10 し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー21（レコーダ2の機器またはアプリケーション）がMKBによってリボーカされたと判定される。レコーダ2は、以後の処理を中断し、DVDメディア1への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

15 レコーダ2は、DVDメディア1からメディアID11を読み、メディアキーと共にメディアIDをC2_G23に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器24で発生させたタイトルキーがC2_E25で暗号化され、暗号化タイトルキー14としてDVDメディア1に記録される。タイトルキーとコンテンツのCCI情報がC2_G26で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをC2_ECBC27で暗号化し、DVDメディア1上に暗号化コンテンツ13としてCCI15と共に記録する。

プレーヤ3による再生の手順について説明する。最初にMKB12をDVDメディア1から読み出す。デバイスキー31とMKB12を演算し、リボケーションの確認がなされる。デバイスキー31、すな

わち、プレーヤ3の機器またはアプリケーションがリポートされない場合には、メディアIDを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー14とメディアユニークキーからタイトルキーが演算される。タイトルキーとCC115とがC2_G
5 36に入力され、コンテンツキーが導出される。コンテンツキーがC2_DCB
C37に入力され、コンテンツキーを鍵として、DVDメディア1から再生された暗号化コンテンツ13に対してC2_DCB
C37の演算が施される。その結果、暗号化コンテンツ13が復号される。

10 このように、コンテンツの復号に必要なコンテンツキーを得るために、DVDメディアの1枚毎に異なるメディアIDが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアIDがオリジナルのメディアIDと異なるために、コピーされたコンテンツを復号することができ
15 ず、コンテンツの著作権を保護することができる。

上述した第1図の構成は、記録再生機器として構成されたものである。この発明は、DVDメディア1に対するコンテンツ保護処理をPC環境下で扱う場合に適用される。第2図を参照して現行の方式によるPCとドライブの役割分担を示す。第2図において、参照符号4が
20 上述したCPRM規格に準拠したDVDメディア1を記録および再生する記録再生装置としてのDVDドライブを示す。

参照符号5がデータ処理装置としてのホスト例えばPCを示す。ホスト5は、DVDメディア1に記録可能で、DVDメディア1から再生可能なコンテンツを扱うことができ、且つDVDドライブ4と接続
25 されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばPCに対してアプリケーションソフトウェアがインス

トールされることによってホスト 5 が構成される。

DVD ドライブ 4 とホスト 5 との間がインターフェース 4 a で接続されている。インターフェース 4 a は、ATAPI (AT Attachment with Packet Interface) , SCSI (Small Computer System Interface) , USB (Universal Serial Bus) , IEEE (Institute of Electrical and Electronics Engineers) 1394 等である。

DVD メディア 1 には、メディア ID 11 、メディアキーブロック 12 および ACC (Authentication Control Code) が予め記録されている。ACC は、DVD ドライブ 4 とホスト 5 との間の認証が DVD 10 メディア 1 によって異なるようにするために予め DVD メディア 1 に記録されたデータである。

DVD ドライブ 4 は、ACC16 を DVD メディア 1 から読み出す。DVD メディア 1 から読み出された ACC16 が DVD ドライブ 4 の AKE (Authentication and Key Exchange) 41 に入力されると共 15 に、ホスト 5 へ転送される。ホスト 5 は、受け取った ACC を AKE 51 に入力する。AKE 41 および 51 は、乱数データを交換し、この交換した乱数と ACC の値とから認証動作の度に異なる値となる共通のセッションキー (バスキーと称する) を生成する。

バスキーが MAC (Message Authentication Code) 演算ブロック 4 20 2 および 52 にそれぞれ供給される。MAC 演算ブロック 42 および 52 は、AKE 41 および 51 でそれぞれ得られたバスキーをパラメータとして、メディア ID および メディアキーブロック 12 の MAC を計算するプロセスである。MKB とメディア ID の完全性 (integrity) をホスト 5 が確認するために利用される。

25 MAC 42 および 52 によってそれぞれ計算された MAC がホスト 5 の比較 53 において比較され、両者の値が一致するかどうかが判定

される。これらのM A Cの値が一致すれば、M K BとメディアI Dの完全性が確認されたことになる。比較出力でスイッチS W 1が制御される。

スイッチS W 1は、D V Dドライブ4のD V Dメディア1の記録または再生経路と、ホスト5の暗号化／（または）復号モジュール5 4との間の信号路をON／OFFするものとして示されている。スイッチS W 1は、信号路のON／OFFを行うものとして示されているが、より実際には、ONの場合にホスト5の処理が継続し、OFFの場合にホスト5の処理が停止することを表している。暗号化／復号モジュール5 4は、メディアユニークキーと暗号化タイトルキーとC C Iとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ1 3へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ1 3を復号する演算ブロックである。

メディアユニークキー演算ブロック5 5は、M K B 1 2とメディアI Dとデバイスキー5 6とからメディアユニークキーを演算する演算ブロックである。第1図に示すレコーダまたはプレーヤと同様に、デバイスキーとM K B 1 2とからメディアキーが演算される。メディアキーとメディアI D 1 1とからメディアユニークキーが演算される。

メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボーケーションを行なうリボーケーション部としての機能も有する。

記録時に、比較5 3によって完全性が確認された場合には、スイッチS W 1がONされる。暗号化／復号モジュール5 4からスイッチS W 1を通じてドライブ4に対して、暗号化コンテンツ1 3、暗号化タイトルキー1 4およびC C I 1 5が供給され、D V Dメディア1に対

してそれぞれ記録される。再生時に、比較 5 3 によって完全性が確認された場合には、スイッチ SW 1 が ON される。DVD メディア 1 からそれぞれ再生された暗号化コンテンツ 1 3 、暗号化タイトルキー 1 4 および CCI 1 5 がスイッチ SW 1 を通じてホスト 5 の暗号化／復号モジュール 5 4 に対して供給され、暗号化コンテンツが復号される。

第 3 図は、第 2 図に示す現行の PC 環境下の DVD メディアを利用するシステムにおいて、DVD メディア 1 と、DVD ドライブ 4 と、ホスト 5 との間の信号の授受の手順を示す。ホスト 5 が DVD ドライブ 4 に対してコマンドを送り、DVD ドライブ 4 がコマンドに応答した動作を行う。

ホスト 5 からの要求に応じて DVD メディア 1 上の ACC がシークされ、読み出される（ステップ S 1）。次のステップ S 2 において、読み出された ACC が AKE 4 1 に入力されると共に、ホスト 5 へ転送され、ホスト 5 では、受け取った ACC が AKE 5 1 へ入力される。AKE 4 1 および 5 1 は、乱数データを交換し、この交換した乱数と ACC 1 6 の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーを DVD ドライブ 4 とホスト 5 が共有する。相互認証が成立しなかった場合では、処理が中断する。

認証動作は、電源の ON または OFF 時並びにディスクの交換時には、必ず行われる。記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

認証が成功すると、ステップ S 3 において、ホスト 5 が DVD ドライブ 4 に対して、DVD メディア 1 からの MKB (メディアキーブロ

ック) パック#0 の読み出しを要求する。MKB は、パック0～パック15 の16セクタが12回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

DVD ドライブ4 がステップS4 においてMKB のパック#0 を読みに行き、ステップS5 において、パック#0 が読み出される。DVD ドライブ4 は、モディファイドMKB をホスト5 へ戻す(ステップS6)。MKB を読み出す際に、バスキーをパラメータとしてMAC 値を計算し、MKB に対してMAC 値を付加してホスト5 へデータを転送する。パック#0 以外の残りのMKB パックの要求と、DVD ドライブ4 の読み出し動作と、モディファイドMKB パックの転送動作とがMKB のパックがなくなるまで、例えばパック#15 が読み出され、ホスト5 へ転送されるまで、ステップS7 およびS8 によって繰り返しなされる。

ホスト5 がDVD ドライブ4 に対してメディアID を要求する。DVD ドライブ4 がDVD メディア1 に記録されているメディアID を読みに行き、ステップS11 において、メディアID が読み出される。DVD ドライブ4 は、メディアID を読み出す際に、バスキーをパラメータとしてそのMAC 値を計算する。DVD ドライブ4 は、ステップS12 において、読み出されたメディアID に対してMAC 値m1 を付加してホスト5 へデータを転送する。

ホスト5 では、DVD ドライブ4 から受け取ったMKB12 およびメディアID11 からバスキーをパラメータとして再度MAC 値を計算し、計算したMAC 値とDVD ドライブ4 から受け取ったMAC 値とを比較53 で比較する。両者が一致したならば、正しいMKB およびメディアID を受け取ったと判定して、スイッチSW1 をON に設定して処理を先に進める。逆に両者が一致しなかったならば、MKB

およびメディア I D が改ざんされたものと判定して、スイッチ SW 1 を OFF に設定して処理を中断する。

ステップ S 1 3 において、ホスト 5 が D V D ドライブ 4 に対して暗号化コンテンツを要求し、ステップ S 1 4 において、 D V D ドライブ 5 4 が暗号化コンテンツを読み出し、ステップ S 1 3 において、読み出した暗号化コンテンツがホスト 5 に転送される。ホスト 5 のメディアユニークキー演算ブロック 5 5 では、デバイスキー 5 6 と M K B 1 2 とメディア I D 1 1 とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール 5 4 に供給され、暗号化タイトルキー 1 4 、 C C I 1 5 からコンテンツキーが求められる。コンテンツキーを鍵として D V D メディア 1 から読み出された暗号化コンテンツが復号される。 D V D メディア 1 に対して記録されるコンテンツが暗号化される。

第 4 図のフローチャートにおいて、ステップ S T 1 は、 M A C 演算ブロック 4 2 でバスキーをパラメータとして求められた M A C 計算値と、 M A C 演算ブロック 5 3 でバスキーをパラメータとして求められた M A C 計算値とを比較するステップである。両者が一致すれば、スイッチ SW 1 がステップ S T 2 において ON とされる。両者が一致しない場合では、スイッチ SW 1 がステップ S T 3 において OFF とされ、処理が停止する。

第 2 図に示すような P C 環境下のシステムに対して適用されるこの発明の第 1 の実施形態を第 5 図に示す。第 1 の実施形態は、ホスト 5 の側で秘密情報とされているデバイスキーを D V D ドライブ 4 側に記憶するようにしたものである。デバイスキーは、上述したように、リモートボーケーション動作とメディアキーの導出に使用される情報である。

第 5 図において、参照符号 4 6 が D V D ドライブ 4 側に記憶された

デバイスキーである。デバイスキー 4 6 をセキュアにホスト 5 に伝送するために、デバイスキー 4 6 が暗号化例えは D E S (Data Encryption Standard) エンクリプタ 4 7 に入力され、バスキーで暗号化される。暗号化デバイスキーがドライブホストインターフェース 4 a を通じてホスト 5 へ転送される。

比較 5 3 において M A C 値が一致すると検出された場合、すなわち、完全性が確認できた場合にのみ O N するスイッチ S W 2 を介して暗号化デバイスキーが D E S デクリプタ 5 7 に入力される。スイッチ S W 2 は、信号路の O N / O F F を行うものとして示されているが、より実際には、スイッチ S W 1 と同様に、 O N の場合にホスト 5 の処理が継続し、 O F F の場合にホスト 5 の処理が停止することを表している。D E S デクリプタ 5 7 には、バスキーが供給され、デバイスキーが復号される。

復号されたデバイスキーがメディアユニークキー演算ブロック 5 5 に供給され、 M K B 1 2 とメディア I D とデバイスキー 4 6 とからメディアユニークキーが演算される。 M K B 1 2 とデバイスキー 4 6 とを使用してメディアキーが計算され、メディア I D とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキー演算ブロック 5 5 において、計算されたメディアキーが所定の値となる場合には、デバイスキー、すなわち、 D V D ドライブ 4 がリボークされ、処理が停止される。メディアユニークキー演算ブロック 5 5 は、リボーク処理部の機能を有している。

メディアユニークキーが暗号化／復号モジュール 5 4 に供給され、暗号化タイトルキー 1 4 、 C C I 1 5 からコンテンツキーが求められる。コンテンツキーを使用して D V D メディア 1 から読み出された暗号化コンテンツが復号され、 D V D メディア 1 に対して記録されるコ

ンテンツが暗号化される。

第6図は、第1の実施形態の処理の手順を示す。ACCのシークおよびリード（ステップS21）からメディアIDとm1をリターン（ステップS32）までの処理は、第3図に示すものと同様であるので5、この処理については、簡単に説明する。ステップS21では、ACCがシークされ、読み出され、ステップS22において認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。

ステップS23において、ホスト5がMKB（メディアキープロック）パック#0の読み出しをDVDドライブ4に要求し、DVDドライブ4がステップS24においてMKBパック#0を読みに行き、ステップS25において、パック#0が読み出される。ステップS26で、DVDドライブ4は、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を附加したデータ（モディファイドMKB）をホスト5へ戻す。ステップS27およびS28において、パック#0以外の残りのMKBパックの要求と、読み出し動作と、転送動作とがなされる。

ホスト5がメディアIDを要求し（ステップS29）、DVDドライブ4がメディアIDを読みに行き（ステップS30）、ステップS2031において、メディアIDが読み出される。DVDドライブ4は、メディアIDを読み出す際に、バスキーをパラメータとしてそのMAC値を計算し、ステップS32において、読み出されたメディアIDに対してMAC値m1を附加してホスト5へデータを転送する。

ホスト5では、DVDドライブ4から受け取ったMKB12および25メディアID11からバスキーをパラメータとして再度MAC値を計算する。計算したMAC値とDVDドライブ4から受け取ったMAC

値とが一致したならば、正しいMKBおよびメディアIDを受け取ったと判定して、スイッチSW1をONに設定して処理を先に進める。逆に両者が一致しなかったならば、MKBおよびメディアIDが改ざんされたものと判定して、スイッチSW1をOFFに設定して処理を5停止する。

ステップS33において、ホスト5がDVDドライブ4に対してデバイスキーを要求する。DVDドライブ4は、デバイスキー46をDESエンクリプタ47によって暗号化し、暗号化デバイスキーをホスト5に送る（ステップS34）。ホスト5は、バスキーを使用してDESデクリプタ57によってデバイスキーを復号する。

ステップS35において、ホスト5がDVDドライブ4に対して暗号化コンテンツを要求し、ステップS36において、DVDドライブ4が暗号化コンテンツを読み出し、ステップS35において、読み出した暗号化コンテンツがホスト5に転送される。ホスト5のメディアユニークキー演算ブロック55では、デバイスキー46とMKB12とメディアID11とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール54に供給され、暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

20 上述した第1の実施形態では、著作権保護技術に関する秘密情報であるデバイスキーがDVDドライブ4内に実装されている。例えばフラッシュメモリ等のLSI (Large Scale Integrated Circuit : 大規模集積回路) 内にデバイスキーが実装される。LSI内のデバイスキーを外部から読み取ることが不可能とされている。ホスト5にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアの

リバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

DVDメディア1を扱う正当なドライブとなるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりますのようなクローン・ドライブの作成を防止できる効果がある。

PC環境下で実施されるこの発明の第2の実施形態を第7図に示す。第2の実施形態は、ホスト5の側で秘密情報とされているデバイスキーを二つの要素に分解し、その内の方の要素をDVDドライブ4側に記憶するようにしたものである。

第7図において、参照符号46aがDVDドライブ4側に記憶されたデバイスキーの前半部である。デバイスキーの前半部とは、デバイスキーの後半部と組み合わされることによって完全なデバイスキーを構成するデバイスキーの一部分のことである。デバイスキーの前半部46aが暗号化例えはDESエンクリプタ47に入力され、バスキーで暗号化される。暗号化デバイスキーの前半部がドライブホストインターフェース4aを通じてホスト5へ転送される。

比較53においてMAC値が一致すると検出された場合にのみONするスイッチSW2を介して暗号化デバイスキーの前半部がDESデクリプタ57に入力される。DESデクリプタ57には、バスキーが供給され、デバイスキーの前半部がDESデクリプタ57によって復号される。

参照符号56aがデバイスキーの後半部を示す。DESデクリプタ57によって復号されたデバイスキーの前半部46aとデバイスキーの後半部56aとがデバイスキー合成部58に入力され、両者が合成されることで、デバイスキーが得られる。

得られたデバイスキーがメディアユニークキー演算ブロック 5 5 に供給され、MKB 1 2 とメディアIDとデバイスキー 4 6 とからメディアユニークキーが演算される。そして、メディアユニークキーが暗号化／復号モジュール 5 4 に供給される。暗号化タイトルキー 1 4 、
5 CCI 1 5 からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア 1 から読み出された暗号化コンテンツが復号され、また、DVDメディア 1 に対して記録されるコンテンツが暗号化される。

上述した第 2 の実施形態は、デバイスキーを二つの要素に分解して
10 いる点を除くと、第 1 の実施形態と同様のものであり、処理の手順は、第 6 図と同様のものであり、その図示については省略する。

第 2 の実施形態では、著作権保護技術に関するデータとしてデバイスキーの一部がドライブ 4 内に実装されている。例えばLSI 内にデバイスキーの一部が実装される。その結果、ホスト 5 にインストール
15 されるアプリケーションは、著作権保護技術に関するデータを一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

DVDメディア 1 を扱う正当なドライブとなるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりますのようなクローン・ドライブの作成を防止できる効果がある。デバイスキーの前半部 4 6 a とその後半部 5 6 a が共に正しい場合にのみ、電子機器またはアプリケーションソフトウェアが正当なものとされるので、DVD ドライブ 4 およびホスト 5 の両方について、リポート処理を行うことが可能となる。

第8図は、この発明の第3の実施形態を示す。第3の実施形態では、デバイスキ-46をDVDドライブ4が持ち、参照符号48で示すメディアユニークキー演算ブロックをDVDドライブ4が持つようにしたものである。

5 第3の実施形態では、メディアユニークキー演算ブロック48がDVDドライブ4に設けられているので、DVDメディア1から再生されたMKBおよびメディアIDをホスト5へ転送することが不要となる。その結果、MAC演算ブロック、計算されたMAC値の比較および比較出力で制御されるスイッチが不要となる。リボケーションもホ
10 10 スト5に依存することがなくなり、DVDメディア1とDVDドライブ4だけで処理が完結するようになる。

DVDドライブ4に設けられたメディアユニークキー演算ブロック48において、MKB12とメディアIDとデバイスキ-46とからメディアユニークキーが演算される。MKB12とデバイスキ-46
15 15 とを使用してメディアキーが計算され、メディアID11とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキーをセキュアにホスト5に伝送するために、メディアユニークキーがDESエンクリプタ49に供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト5のDESデ
20 20 クリプタ59に供給され、バスキーを使用して復号される。

復号されたメディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対し
25 25 て記録されるコンテンツが暗号化される。

第9図は、第3の実施形態の処理の手順を示す。ACCのシークお

よびリード（ステップS41）から残りのMKBパックのリード（ステップS48）までの処理は、第3図に示すものと同様であるので、この処理については、簡単に説明する。

ステップS42では、認証が行われ、認証が成功すると、認証動作5の度に異なる値となるセッションキーとしてのバスキーが生成される。ステップS43において、ホスト5がMKB（メディアキーブロック）パック#0の読み出しをDVDドライブ4に要求し、DVDドライブ4がステップS44においてMKBパック#0を読みに行き、ステップS45において、パック#0が読み出される。ステップS4610で、DVDドライブ4は、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加したデータをホスト5へ転送する。ステップS47およびS48において、パック#0以外の残りのMKBパックの要求と、読み出し動作と、転送動作とがなされる。

ステップS49において、ホスト5がメディアユニークキーを要求15すると、DVDドライブ4が暗号化メディアユニークキーをホスト5に送る（ステップS50）。メディアユニークキーが暗号化／復号モジュール54に供給される。ステップS51において、ホスト5が暗号化コンテンツを要求すると、DVDドライブ4が暗号化コンテンツ20をリードし（ステップS52）、暗号化／復号モジュール54によって暗号化コンテンツが復号され、DVDメディア1に対して記録されるコンテンツが暗号化される。

第10図は、この発明の第4の実施形態を示す。第4の実施形態では、第3の実施形態と同様に、メディアユニークキー演算ブロック4258をDVDドライブ4が持ち、ホスト5がデバイスキーアクセスキー56を持ち、ホスト5からDVDドライブ4へデバイスキーアクセスキー56をセキュアに転送

するものである。

第4の実施形態では、メディアユニークキー演算ブロック48がDVDドライブ4に設けられているので、DVDメディア1から再生されたMKBおよびメディアIDをホスト5へ転送することが不要となる。その結果、MAC演算ブロック、計算されたMAC値の比較および比較出力で制御されるスイッチが不要となる。

ホスト5のデバイスキー56がDESエンクリプタ59bに供給され、バスキーを鍵として暗号化される。暗号化デバイスキーがDVDドライブ4のDESデクリプタ49bに転送され、デバイスキーがDVDドライブ4において復号される。復号されたデバイスキーがメディアユニークキー演算ブロック48に入力される。

DVDドライブ4に設けられたメディアユニークキー演算ブロック48において、MKB12とメディアIDとデバイスキー46とからメディアユニークキーが演算される。すなわち、MKB12とデバイスキー46とを使用してメディアキーが計算され、メディアID11とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキーがDESエンクリプタ49aに供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト5のDESデクリプタ59aに供給され、バスキーを使用して復号される。

復号されたメディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

第11図は、第4の実施形態の処理の手順を示す。ACCのシーク

およびリード（ステップ S 6 1）から残りのMKBパックのリード（ステップ S 6 8）までの処理は、第3図に示すものと同様であるので、この処理については、簡単に説明する。

ステップ S 6 2 では、認証が行われ、認証が成功すると、認証動作
5 の度に異なる値となるセッションキーとしてのバスキーが生成される。次に、ステップ S 6 3 において、ホスト 5 がMKB（メディアキー
プロック）パック#0 の読み出しをDVD ドライブ 4 に要求し、DVD
D ドライブ 4 がステップ S 6 4 においてMKB パック#0 を読みに行
き、ステップ S 6 5 において、パック#0 が読み出される。ステップ
10 S 6 6 で、DVD ドライブ 4 は、MKB を読み出す際に、バスキーを
パラメータとして MAC 値を計算し、MKB に対して MAC 値を付加
したデータをホスト 5 へ転送する。ステップ S 6 7 および S 6 8 にお
いて、パック#0 以外の残りのMKB パックの要求と、読み出し動作
と、転送動作とがなされる。

ステップ S 6 9 において、暗号化デバイスキーをホスト 5 がDVD
15 ドライブ 4 に送る。DVD ドライブ 4 において、メディアユニークキー
が演算される。ステップ S 7 0 において、ホスト 5 がメディアユニー
クキーを要求すると、DVD ドライブ 4 が暗号化メディアユニーク
キーをホスト 5 に送る（ステップ S 7 1）。メディアユニークキーが
20 暗号化／復号モジュール 5 4 に供給される。ステップ S 7 2 におい
て、ホスト 5 が暗号化コンテンツを要求すると、DVD ドライブ 4 が暗
号化コンテンツをリードし（ステップ S 7 3）、暗号化／復号モジュ
ール 5 4 によって暗号化コンテンツが復号され、DVD メディア 1 に
25 対して記録されるコンテンツが暗号化される。

上述した第3 および第4 の実施形態では、著作権保護技術に関する
アルゴリズムの一部例えばメディアユニークキーの演算がドライブ 4

内に実装されている。例えば L S I 内にメディアユニークキー演算ブロック 4 8 が実装される。ホスト 5 にインストールされるアプリケーションは、著作権保護技術に関するアルゴリズムの一部しか持たないで良い。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

第 3 の実施形態では、D V D メディア 1 を扱う正当なドライブとなるために、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりますよ
10 うなクローン・ドライブの作成を防止できる効果がある。

第 1 2 図は、この発明の第 5 の実施形態を示す。上述した第 1 ～第 4 の実施形態では、D V D の著作権保護技術である C P R M に対してこの発明を適用したものである。第 5 の実施形態は、第 2 図に示す実際に運用されている C P R M のアーキテクチャを拡張した構成を有す
15 る。

第 5 の実施形態は、ホスト 5 のメディアユニークキー演算ブロック 6 1 に対して、パラメータ A 6 2 が関与し、暗号化／復号モジュール 6 3 に対して、パラメータ B 6 4 が関与するようにしたものである。パラメータ A 6 2 およびパラメータ B 6 4 は、固定値および D V D メ
20 ディア 1 から読み出されたデータの何れであっても良い。

現行の C P R M では、M K B とデバイスキーからメディアキーを計算し、メディアキーとメディア I D からメディアユニークキーを計算している。C P R M を拡張したシステムにおいては、この計算の過程で、パラメータ A 6 2 が関与し、暗号化／復号モジュール 6 3 では、
25 コンテンツキーを計算する時に、パラメータ B 6 4 が関与する。第 5 の実施形態の処理の手順は、現行の C P R M と同様のものであり、そ

の図示については省略する。

第13図は、この発明の第6の実施形態を示す。第6の実施形態は、実際に運用されているCPRMのアーキテクチャを拡張した構成を有し、デバイスキー46と、パラメータA62と、パラメータB64とをDVDドライブ4が持つようにしたものである。これらのデバイスキー46、パラメータA62およびパラメータB64をセキュアにホスト5に伝送するために、DESエンクリプタ65でこれらの情報がバスキーで暗号化される。

比較53においてMAC値が一致すると検出された場合、すなわち10、完全性が確認できた場合にのみONするスイッチSW3を介して暗号化されたデータがDESデクリプタ66に入力される。DESデクリプタ66には、バスキーが供給され、デバイスキー、パラメータA62およびパラメータB64が復号される。復号されたデバイスキーおよびパラメータAがメディアユニークキー演算ブロック61に供給15され、MKB12とメディアIDとデバイスキー46とパラメータAとからメディアユニークキーが演算される。

メディアユニークキーおよびパラメータBが暗号化／復号モジュール63に供給され、これらのデータを使用してコンテンツキーが求められ、コンテンツキーを使用してコンテンツの暗号化／復号がなされ20る。

第14図は、第6の実施形態の処理の手順を示す。ACCのシークおよびリード（ステップS81）からメディアIDとm1をリターン（ステップS92）までの処理は、現行のCPRMの処理と同様であるので、この処理については、簡単に説明する。ステップS81では25、ACCがシークされ、読み出され、ステップS82において認証が成功すると、認証動作の度に異なる値となるセッションキーとしての

バスキーが生成される。

ステップ S 8 3において、ホスト 5 がMKB（メディアキープロック）パック#0 の読み出しをDVD ドライブ 4 に要求し、DVD ドライブ 4 がステップ S 8 4 においてMKB パック#0 を読みに行き、
5 テップ S 8 5 において、パック#0 が読み出される。ステップ S 8 6 で、DVD ドライブ 4 は、MKB を読み出す際に、バスキーをパラメータとしてMAC 値を計算し、MKB に対してMAC 値を付加したデータ（モディファイドMKB）をホスト 5 へ戻す。ステップ S 8 7 および S 8 8 において、パック#0 以外の残りのMKB パックの要求と
10 、読み出し動作と、転送動作とがなされる。

ホスト 5 がメディア ID を要求し（ステップ S 8 9 ）、DVD ドライブ 4 がメディア ID を読みに行き（ステップ S 9 0 ）、ステップ S 9 1 において、メディア ID が読み出される。DVD ドライブ 4 は、
15 メディア ID を読み出す際に、バスキーをパラメータとしてそのMAC 値を計算し、ステップ S 9 2 において、読み出されたメディア ID に対してMAC 値m1 を付加してホスト 5 へデータを転送する。

ホスト 5 では、DVD ドライブ 4 から受け取ったMKB 1 2 および
メディア ID 1 1 からバスキーをパラメータとして再度MAC 値を計算する。計算したMAC 値とDVD ドライブ 4 から受け取ったMAC
20 値とが一致したならば、正しいMKB およびメディア ID を受け取ったと判定して、スイッチ SW1 およびスイッチ SW3 をON に設定して処理を先に進める。逆に両者が一致しなかったならば、MKB およびメディア ID が改ざんされたものと判定して、スイッチ SW1 およびスイッチ SW3 をOFF に設定して処理を停止する。
25 テップ S 9 3 において、ホスト 5 がDVD ドライブ 4 に対してデータキーとパラメータ A とパラメータ B とを要求する。DVD ドラ

イブ 4 は、デバイスキー 4 6 とパラメータ A とパラメータ B とを D E S エンクリプタ 6 5 によって暗号化し、暗号化データをホスト 5 に送る（ステップ S 9 4）。ホスト 5 は、バスキーを使用して D E S デクリプタ 6 6 によってデバイスキーを復号する。

5 ステップ S 9 5 において、ホスト 5 が D V D ドライブ 4 に対して暗号化コンテンツを要求し、ステップ S 9 6 において、D V D ドライブ 4 が暗号化コンテンツを読み出し、ステップ S 9 5 において、読み出した暗号化コンテンツがホスト 5 に転送される。ホスト 5 のメディアユニークキー演算ブロック 6 1 では、デバイスキー 4 6 と M K B 1 2
10 とメディア I D 1 1 とパラメータ A とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール 6 3 に供給され、暗号化コンテンツが復号され、D V D メディア 1 に対して記録されるコンテンツが暗号化される。

第 1 5 図は、この発明の第 7 の実施形態を示す。第 7 の実施形態では、メディアユニークキー演算ブロック 6 7 を D V D ドライブ 4 が持ち、ホスト 5 がデバイスキー 5 6 とパラメータ A 6 2 とパラメータ B 6 4 とを持ち、ホスト 5 から D V D ドライブ 4 へデバイスキー 5 6 およびパラメータ A 6 2 をセキュアに転送するものである。

第 7 の実施形態では、メディアユニークキー演算ブロック 6 7 が D V D ドライブ 4 に設けられているので、D V D メディア 1 から再生された M K B およびメディア I D をホスト 5 へ転送することが不要となる。その結果、M A C 演算ブロック、計算された M A C 値の比較および比較出力で制御されるスイッチが不要となる。

ホスト 5 のデバイスキー 5 6 およびパラメータ A 6 2 が D E S エンクリプタ 6 8 に供給され、バスキーを鍵として暗号化される。暗号化データが D V D ドライブ 4 の D E S デクリプタ 6 9 に転送され、デバ

イスキーおよびパラメータ A が DVD ドライブ 4 において復号される。復号されたデバイスキーおよびパラメータ A がメディアユニークキー演算ブロック 6 7 に入力される。

DVD ドライブ 4 に設けられたメディアユニークキー演算ブロック 5 6 7 において、MKB 1 2 とメディア ID とデバイスキー 4 6 とパラメータ A とからメディアユニークキーが演算される。メディアユニークキーが DES エンクリプタ 7 0 に供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト 5 の DES デクリプタ 7 1 に供給され、バスキーを使用して復号される。

10 復号されたメディアユニークキーが暗号化／復号モジュール 6 3 に供給され、暗号化タイトルキー 1 4 、 CCI 1 5 およびパラメータ A からコンテンツキーが求められる。コンテンツキーを使用して DVD メディア 1 から読み出された暗号化コンテンツが復号され、また、 DVD メディア 1 に対して記録されるコンテンツが暗号化される。

15 第 1 6 図は、第 7 の実施形態の処理の手順を示す。ACC のシークおよびリード（ステップ S 1 0 1 ）から残りの MKB パックのリード（ステップ S 1 0 8 ）までの処理は、現行の CPRM の処理と同様であるので、この処理については、簡単に説明する。

ステップ S 1 0 2 では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。ステップ S 1 0 3 において、ホスト 5 が MKB （メディアキープロック）パック # 0 の読み出しを DVD ドライブ 4 に要求し、 DVD ドライブ 4 がステップ S 1 0 4 において MKB パック # 0 を読みに行き、ステップ S 1 0 5 において、パック # 0 が読み出される。ステップ S 1 0 6 で、 DVD ドライブ 4 は、 MKB を読み出す際に、バスキーをパラメータとして MAC 値を計算し、 MKB に対して MAC 値を

付加したデータをホスト 5 へ転送する。ステップ S 107 および S 108 において、パック#0 以外の残りの M K B パックの要求と、読み出し動作と、転送動作とがなされる。

ステップ S 109 において、暗号化デバイスキーおよび暗号化パラメータをホスト 5 が D V D ドライブ 4 に送る。ステップ S 110 において、ホスト 5 がメディアユニークキーを要求する。D V D ドライブ 4 において、メディアユニークキーが演算される。ステップ S 111 において、D V D ドライブ 4 が暗号化メディアユニークキーをホスト 5 に送る。メディアユニークキーが暗号化／復号モジュール 63 に供給される。ステップ S 112 において、ホスト 5 が暗号化コンテンツを要求すると、D V D ドライブ 4 が暗号化コンテンツをリードし（ステップ S 113）、暗号化／復号モジュール 63 によって暗号化コンテンツが復号され、D V D メディア 1 に対して記録されるコンテンツが暗号化される。

この発明の第 8 の実施形態について、第 17 図を参照して説明する。第 8 の実施形態は、上述した第 3 の実施形態（第 8 図）と同様に、メディアユニークキーをドライブで生成するものである。第 5 の実施形態（第 12 図）、第 6 の実施形態（第 13 図）または第 7 の実施形態（第 15 図）に示すように、コンテンツキーを生成する場合に関与するパラメータ B を使用するもの（C P R M を拡張したシステム）である。

C P R M を拡張したシステムにおいて、メディアユニークキーを演算するためのパラメータ A と、暗号化／復号のためのパラメータ B とが使用される。これらのパラメータ A, B がホスト側にある場合と、ドライブ側にある場合と、メディアに記録されており、ホストが読み出す場合との全てが可能である。パラメータ A, B をインターフェー

スを介して授受する場合には、暗号化がなされ、セキュアな伝送が必要とされる。

第17図において、参照符号101が記録可能なメディアを示し、
メディア101には、EKB111、暗号化ディスクキーEm(Kd
5)112、暗号化コンテンツ113、ディスクID114およびユニ
ットキー生成用値Vu115が記録されている。第17図では、省略
しているが、暗号化コンテンツ113に関連してCCIが記録されて
いるのは、上述した第1～第7の実施形態例えは第3の実施形態と同
様である。

10 第17図中に記載されている鍵情報に関する用語を下記に説明する
。

EKB111は、各デバイスキーに対してメディアキーKmを配布
するための鍵束である。既述の実施形態におけるメディアキー ブロッ
クMKBに相当する。

15 メディアキーKmは、メディア毎に固有の鍵情報である。EKBの
中にメディアキーが見つからない場合は、そのデバイスキーがリボー
クされたことを示す。

ディスクキーKdは、少なくともコンテンツ毎に異なる鍵情報である。
コンテンツのマスター ディスク毎に異ならせても良い。暗号化デ
20 ィスクキーEm(Kd)112は、メディアキーKmでディスクキー
Kdを暗号化した暗号化鍵で、メディア101に記録されている。暗
号化ディスクキーEm(Kd)112は、ドライブ104において、
個々のメディア毎に異なるエンベディッドキーKeを生成するために
使用される。第5～第7の実施形態におけるパラメータA(ドライブ
25 4においてメディアユニークキーを生成するのに使用されるパラメー
タ)に相当する。

ユニットキー生成用値 V_u 1 1 5 は、暗号化単位（暗号化ユニットと称する）ごとに定義することが可能なパラメータである。各暗号化ユニットは、複数のセクタデータから構成される。ユニットキー生成用値 V_u 1 1 5 は、ホスト 1 0 5 において暗号化コンテンツ 1 1 3 を復号するユニットキー K_u を生成するために使用される。第 5 ～ 第 7 の実施形態におけるパラメータ B （ホスト 5 において暗号化コンテンツ 1 3 を暗号化／復号するために使用されるパラメータ）に相当する。

ディスク I D 1 1 4 は、スタンパ毎に異なる I D である。第 3 の実施形態におけるメディア I D に相当する。

エンベディッドキー K_e は、個々のメディア毎に異なる鍵情報であり、第 3 の実施形態におけるメディアユニークキーに相当する。

ドライブ 1 0 4 が持つデバイスキーキー 1 4 6 と、メディア 1 0 1 が持つ EKB 1 1 1 とに基づいてメディアキー K_m が得られる。メディアキー K_m とメディア 1 0 1 が持つ暗号化ディスクキー E_m (K_d) 1 1 2 とに基づいてディスクキー K_d が得られる。ディスクキー K_d とディスク I D 1 1 4 とに基づいてエンベディッドキー K_e が得られる。

ユニットキー K_u は、暗号化コンテンツ 1 1 3 を暗号化／復号する鍵であり、エンベディッドキー K_e とユニットキー生成用値 V_u とに基づいて得られる。ユニットキー K_u は、上述の実施形態におけるコンテンツキーに相当する。

上述した第 8 の実施形態の動作について処理の流れにしたがって説明する。

最初に AKE 1 4 1 および 1 5 1 による認証がなされる。認証が成功すると、バスキーが生成される。第 1 7 図では省略されているが、

AKE141および151の少なくとも一方に対して認証に関するパラメータが供給されている。

ドライブ104では、メディア101からEKBを読み出し、ドライブ104に供給する。メディア101からのEKBとデバイスキードライブ146がドライブ104のプロセスEKB122で演算され、メディアキーK_mが算出される。演算結果が例えば0になるような場合では、デバイスキーがリポートされる。ドライブ104が有しているデバイスキードライブ146は、例えば機種単位でドライブに与えられる固有の鍵である。

10 ドライブ104が暗号化ディスクキーE_m(K_d)をメディア101から読み出し、AES_D123において、メディアキーK_mによってディスクキーK_dが復号される。AES(Advanced Encryption Standard)は、米国政府がDESに代わる新しい暗号化標準として採用した暗号化方法である。

15 さらに、ドライブ104は、メディア101からディスクID115を読み出し、AES_G148において、ディスクIDとディスクキーK_dを演算し、エンベディッドキーK_eを得る。

ドライブ104とホスト105の認証が完了し、バスキーが得られているならば、ホスト105がドライブ104に対してエンベディッドキーK_eの転送を要求する。

ドライブ104がインターフェース104aを経由してホスト105に対してK_eを転送する際に、AESエンクリプタ149にてバスキーによりK_eを暗号化する。ホスト105は、AESデクリプタ159によって復号を行い、K_eを得る。AESエンクリプタ148およびAESデクリプタ149は、例えばCBC(Cipher Block Chaining)モードの処理を行う。

ホスト 105 は、コンテンツを暗号化ユニット単位で処理する。ホスト 105 は、読み出したい暗号化ユニットのユニットキー生成用値 V_u 115 をドライブ 104 から読み出す。AES_G158において、エンベディッドキー K_e とユニットキー生成用値 V_u とからユニットキー K_u が計算される。
5

ホスト 105 は、読み出したい暗号化コンテンツ 113 中の暗号化ユニットをセクタデータ単位で読み出す。ドライブ 104 は、ホスト 105 に対して読み出したセクタデータを転送する。セクタデータがホスト 105 の暗号化／復号モジュール 154 において、属する暗号化ユニットのユニットキー K_u で復号される。
10

次に、第 18 図を参照してこの発明の第 9 の実施形態について説明する。第 9 の実施形態は、ROM タイプのメディア 110 例えば ROM ディスクを再生する例である。

ROM タイプのメディア 110 には、予めコンテンツが記録されて 15 いる。ホスト 105 では、暗号化の処理が不要となり、復号モジュール 160 が使用される。メディア 110 から読み出された暗号化コンテンツが復号モジュール 160 にて復号され、AV コンテンツが得られる。

ROM タイプのメディア 110 の場合では、メディアキー K_m およびディスクキー K_d がコンテンツ毎に固有の鍵情報である。各コンテンツは、1 または複数の暗号化ユニットから構成される。
20

メディア 110 上にエンベディッドキー生成値 V_e が記録される。エンベディッドキー生成値 V_e は、ディスク製造工場でスタンパー（フォトレジストを現像したディスク原盤またはディスク原盤から最初 25 に作成されたスタンパーを意味する）毎に、記録されたゼロでない値である。物理的ウォーターマークとして、通常のデータ記録とは、別

の手段でディスク上に記録される。

エンベディッドキーK_eは、第3の実施形態におけるメディアユニクキーに相当する。エンベディッドキーK_eを生成するためのエンベディッドキー生成値V_eは、一種のメディアIDである。

5 第9の実施形態も、上述した第8の実施形態と同様の処理を行う。最初にAKE141および151による認証がなされ、バスキーが生成される。読み出されたEKBとデバイスキー146がドライブ104のプロセスEKB122で演算され、メディアキーK_mが算出とりボク処理がなされる。そして、AES_D123において、メディアキーK_mによってディスクキーK_dが復号される。さらに、AES_G148において、エンベディッドキーK_eが得られる。

AESエンクリプタ149にてバスキーによりK_eが暗号化される。ホスト105は、AESデクリプタ159によって復号を行い、K_eを得る。

15 ホスト105は、読み出したい暗号化ユニットのユニットキー生成用値V_u115をドライブ104から読み出し、AES_G158において、ユニットキーK_uが計算される。

ホスト105が要求した暗号化ユニットのセクタデータがホスト105の復号モジュール160において、属する暗号化ユニットのユニットキーK_uで復号される。

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーが記録再生装置内に実装されているので、DVD処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著

作権保護技術の安全性を確保することができる。

電子機器またはアプリケーションソフトウェア固有の情報としてのデバイスキーを記録再生装置とデータ処理装置が分けて持つことによって、記録再生装置およびアプリケーションソフトウェアの両方について、リボーカ処理を行うことが可能となる。

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。したがって、データ処理装置のアプリケーションソフトウェアは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばデバイスキーを二つに分割し、ドライブおよびホストが各デバイスキーを持つことも可能である。メディアユニークキー演算ブロックをドライブが持つ構成も可能である。

暗号化コンテンツををインターフェースを介して授受する場合に、暗号化を行い、セキュアな伝送を行っても良い。AKEに対して認証に関係するパラメータを供給するが、例えば排除すべきもののリストまたは排除すべきでないもののリストを供給するようにしても良い。

産業上の利用可能性

また、上述した説明においては、著作権保護技術としてCPRMおよびCPRMを拡張した例を挙げたが、CPRM以外の著作権保護技術に対してもこの発明を適用することができる。PCベースのシステ

ムに対してこの発明が適用されているが、P C とドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

請求の範囲

1. 記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、
5 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

上記記録媒体固有の第1の情報と上記格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と
10 を有する記録再生装置。

2. 請求の範囲1において、

上記第2の情報の一部が上記格納部に格納され、上記データ処理装置に格納された他の部分と合成されて上記第2の情報が形成されるようにした記録再生装置。

3. 請求の範囲1において、

少なくとも上記格納部に格納された第2の情報と上記記録媒体固有の第1の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボク処理部を有する上記データ処理装置に対して、上記接続部が上記格納部に格納された第2の情報を送る記録再生装置。

4. 請求の範囲3において、

25 上記第2の情報を暗号化して送る記録再生装置。

5. 請求の範囲1において、

上記格納部に格納された第 2 の情報と上記記録媒体固有の第 1 の情報とを用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置。

5 6. 記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 2 の

10 情報が格納される格納部と、

上記記録媒体固有の第 1 の情報と上記格納部に格納された第 2 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

15 少なくとも上記接続部を介して上記データ処理装置から送られ、上記格納部に格納された第 2 の情報と、上記記録媒体固有の第 1 の情報とを用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置。

20 7. 請求の範囲 6 において、

暗号化された上記第 2 の情報を復号する復号手段を有する記録再生装置。

8. 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第

25 2 の情報を有するとともに、記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録

されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

上記接続部を介して上記記録再生装置から送られた、上記記録媒体固有の第1の情報と上記電子機器またはアプリケーションソフトウェア固有の第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部と

を有するデータ処理装置。

9. 請求の範囲8において、

10 上記第2の情報の一部が上記格納部に格納され、上記記録再生装置に格納された他の部分と合成されて上記第2の情報が形成されるようにしたデータ処理装置。

10. 請求の範囲8において、

上記接続部を介して上記記録再生装置から送られた上記第2の情報と、上記記録媒体固有の第1の情報とを用いて、上記第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有するデータ処理装置。

11. 請求の範囲10において、

20 暗号化された上記第2の情報を復号する復号手段を有するデータ処理装置。

12. 請求の範囲8において、

少なくとも上記記録再生装置に格納された第2の情報と、上記記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置

と接続するデータ処理装置。

13. 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報を有する格納部と、

5 記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

上記記録媒体固有の第1の情報と上記格納部に格納された第2の情報10とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部とを有し、

上記格納部に格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置に対して、上記格納部に15格納された第2の情報を送るデータ処理装置。

14. 請求の範囲13において、

上記第2の情報を暗号化して送るデータ処理装置。

15. 記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方が可能であると共に、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報を有する記録再生装置と、

少なくとも格納された上記第2の情報と、上記記録媒体固有の第1の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と

を有する記録再生処理システム。

16. 請求の範囲 15 において、

上記データ処理装置が上記記録媒体固有の第 1 の情報と格納された上記第 2 の情報を用いて、当該格納された第 2 の情報が正当な電子機器 5 またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボク処理部を有する記録再生処理システム。

17. 請求の範囲 15 において、

上記記録再生装置が上記記録媒体固有の第 1 の情報と格納された上記第 2 の情報を用いて、当該格納された第 2 の情報が正当な電子機器 10 またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボク処理部を有する記録再生処理システム。

18. 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報として格納された第 2 の情報を有するとともに、記録媒体固有の 15 第 1 の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と、

格納された上記第 2 の情報と、上記記録媒体固有の第 1 の情報に基づいて生成された鍵を用いてデータの暗号化、または暗号化された 20 データの復号が可能なデータ処理装置とからなり、

格納された上記第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボク処理部を有する上記記録再生装置に対して、上記データ処理装置が上記格納部に格納された第 2 の情報を送る記録再生処理システム。

25 19. 不正な電子機器を無効化するための第 1 の情報と、コンテンツ毎に異なる第 2 の情報と、暗号化単位毎に定義可能な第 3 の情報と

、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

5 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第4の情報が格納される格納部と、

上記第1の情報と上記第4の情報とから当該格納された第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であるかを判定するリポート処理部と、

10 上記リポート処理部で上記第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、上記第1の情報、上記第4の情報、上記第2の情報および上記識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と有する記録再生装置。

15 20. 請求の範囲19において、

上記中間鍵情報に基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う認証部と、

上記認証が成立した場合に形成されるバスキーによって上記中間鍵情報20を暗号化して上記データ処理装置に送出する中間鍵情報暗号化部とを有する記録再生装置。

21. 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第4の情報を有するとともに、不正な電子機器を無効化するための第251の情報と、コンテンツ毎に異なる第2の情報と、暗号化単位毎に定義可能な第3の情報と、スタンパ毎に異なる識別データとが記録され

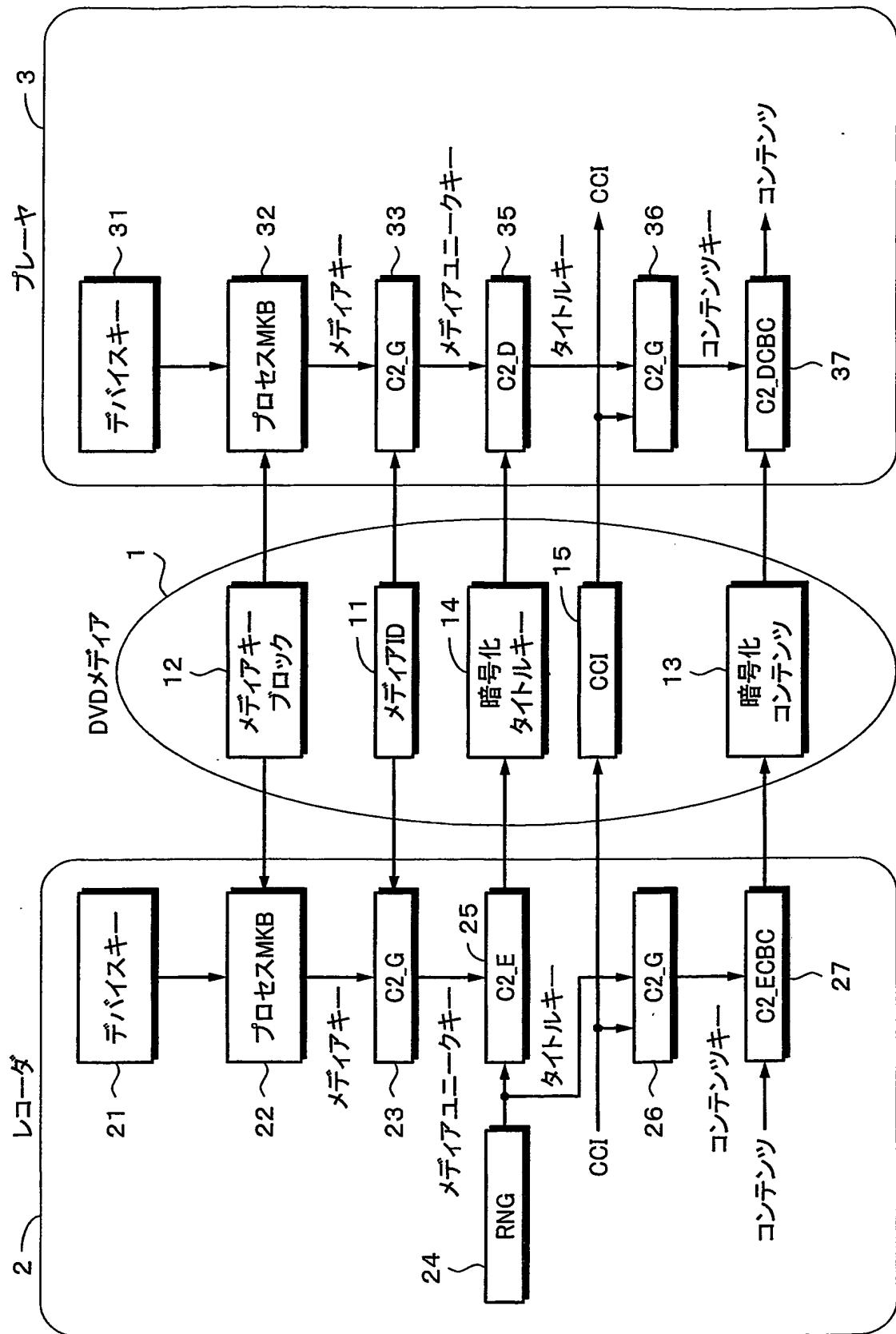
た記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置との認証を行う認証部と、

上記記録再生装置から、上記認証が成立した場合に形成されるバス
5 キーによって暗号化された、上記第1の情報、上記第4の情報、上記
第2の情報および上記識別データから生成された個々の記録媒体毎に
固有の中間鍵情報を受け取り、当該中間鍵情報を復号する鍵情報復号
部と、

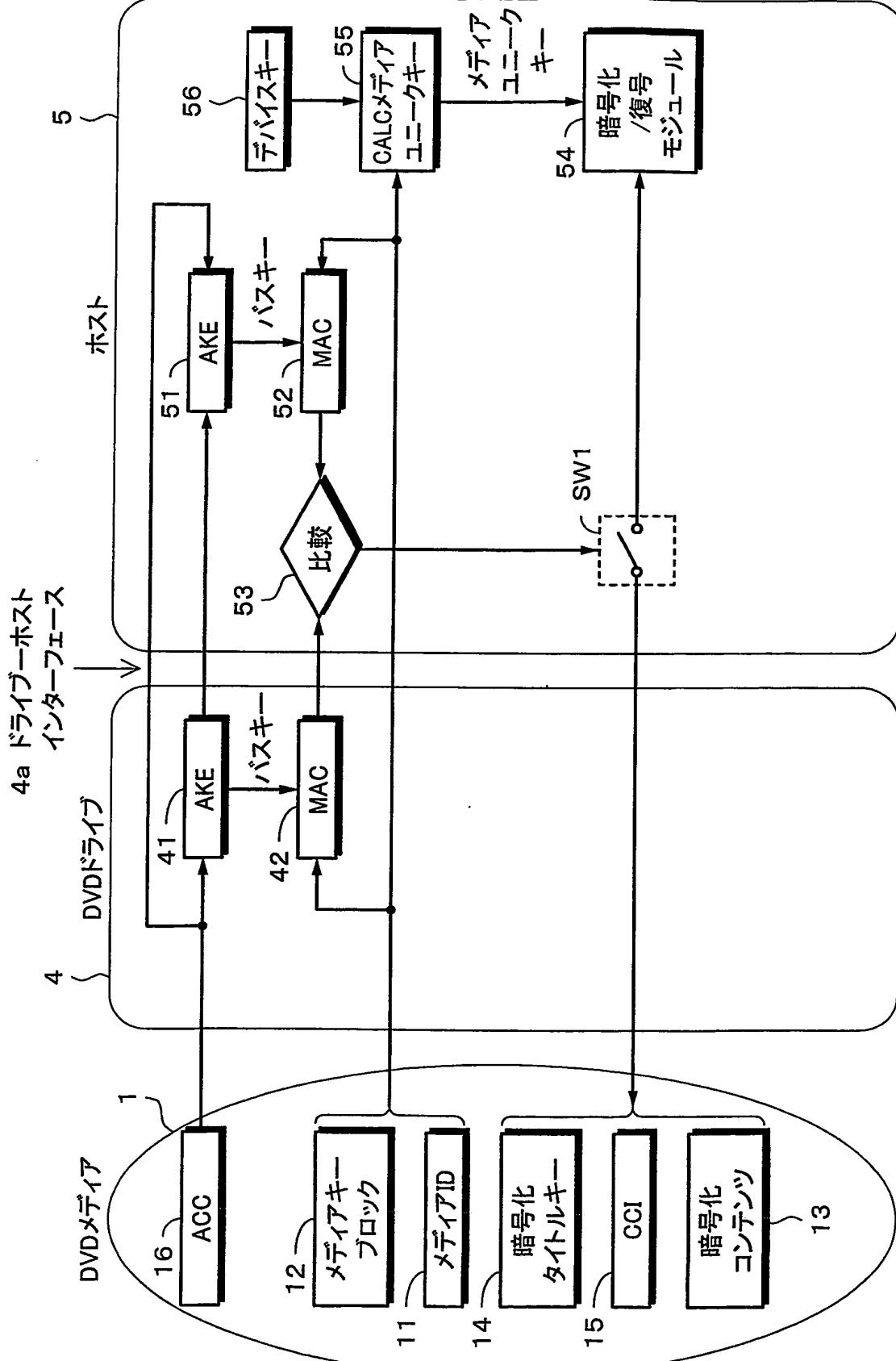
上記記録再生装置から受け取った上記第3の情報と、復号された上
10 記中間鍵情報から暗号化鍵を生成する暗号化鍵生成部と、

上記暗号化鍵による暗号化と上記暗号化鍵による復号との少なくと
も一方を行う暗号化復号部とを有するデータ処理装置。

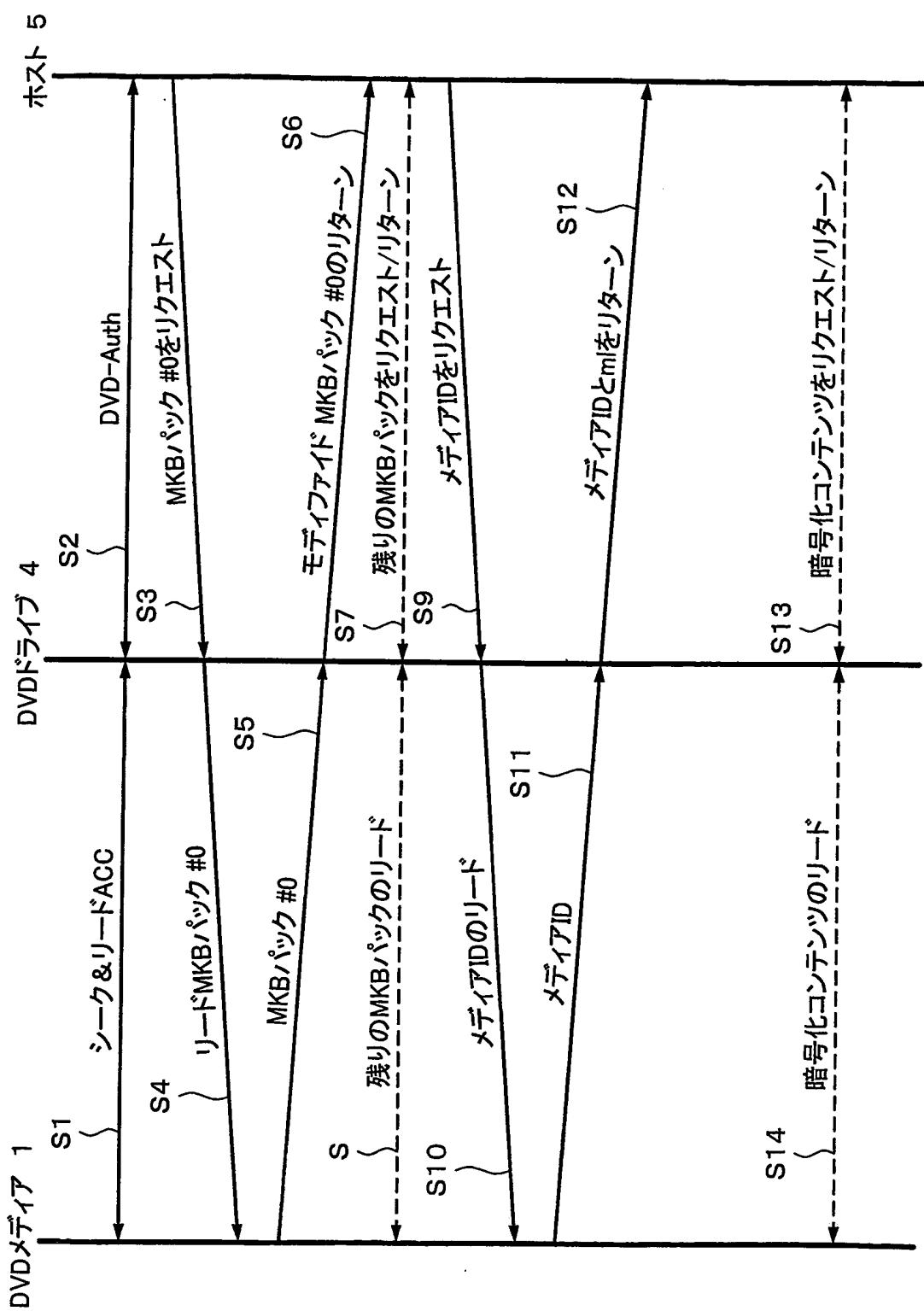
第1図



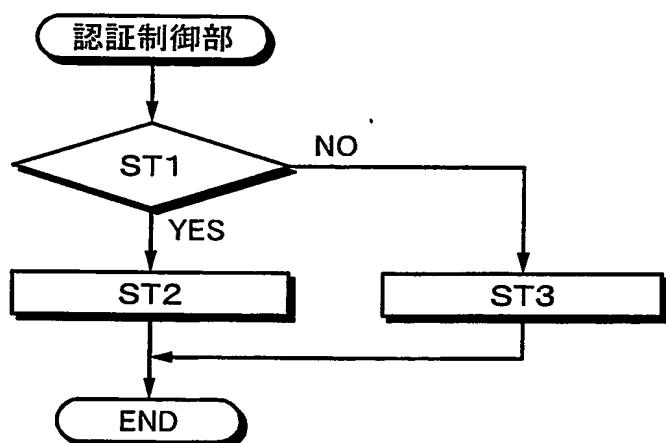
第2図



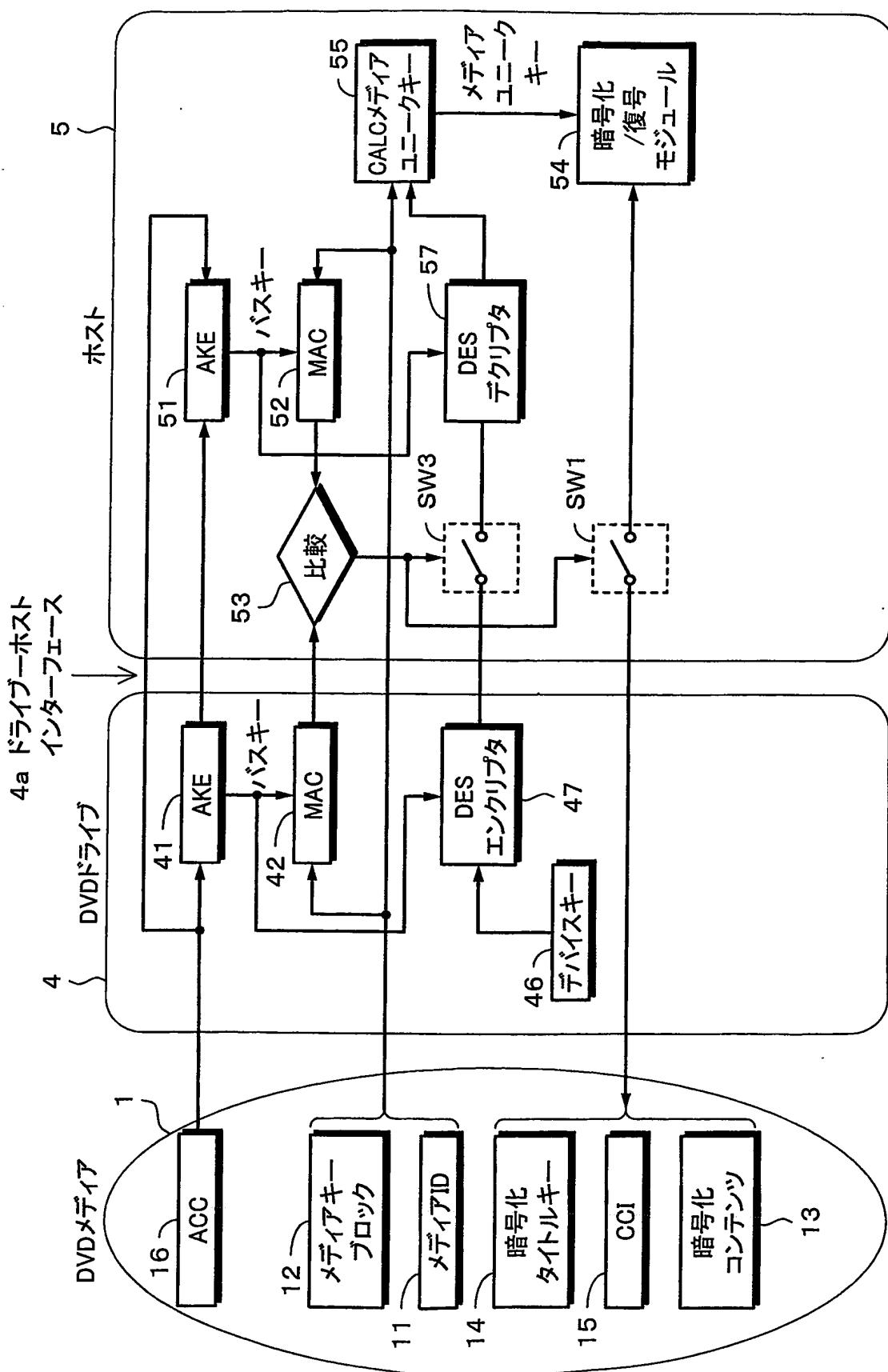
第3図



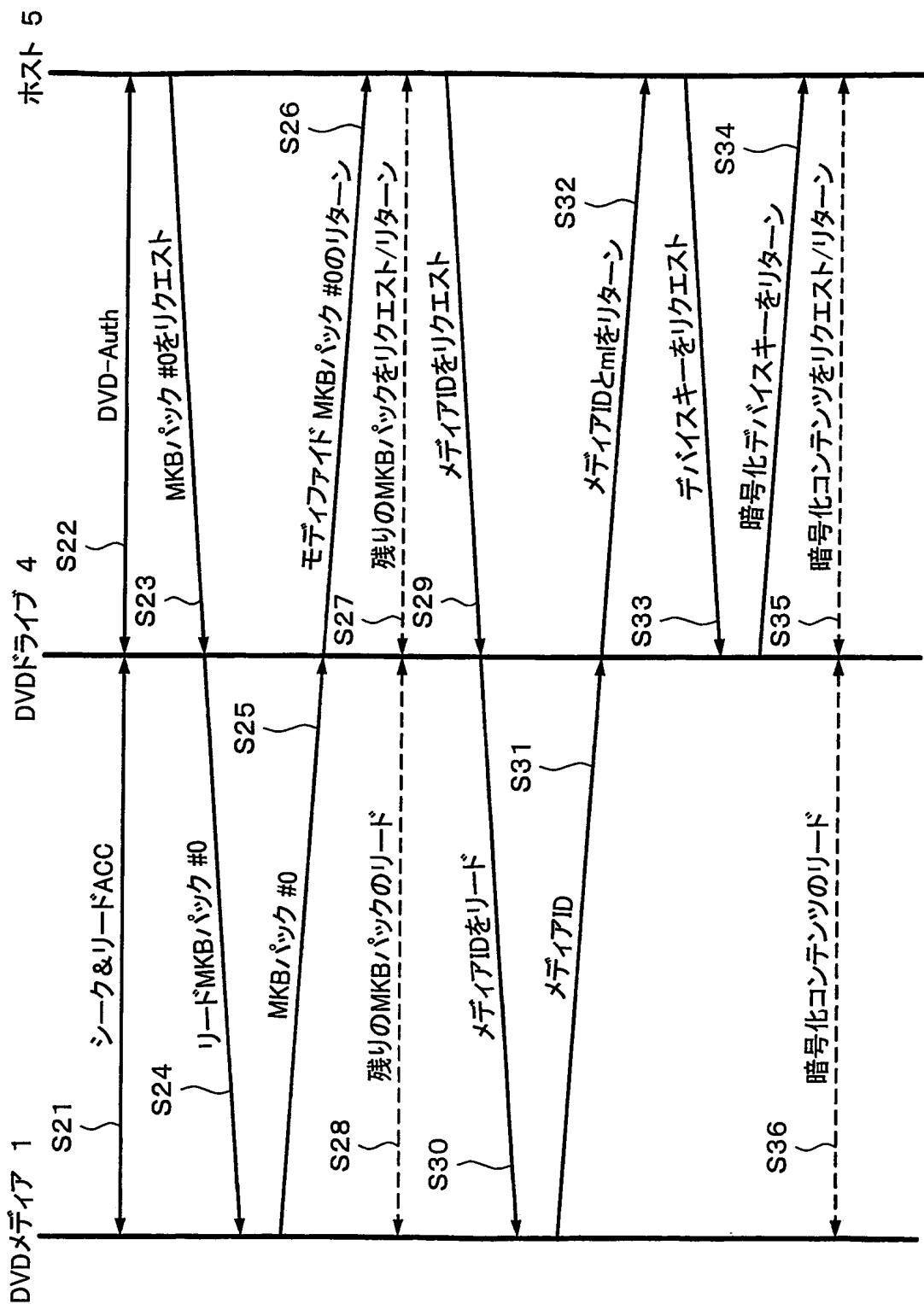
第4図



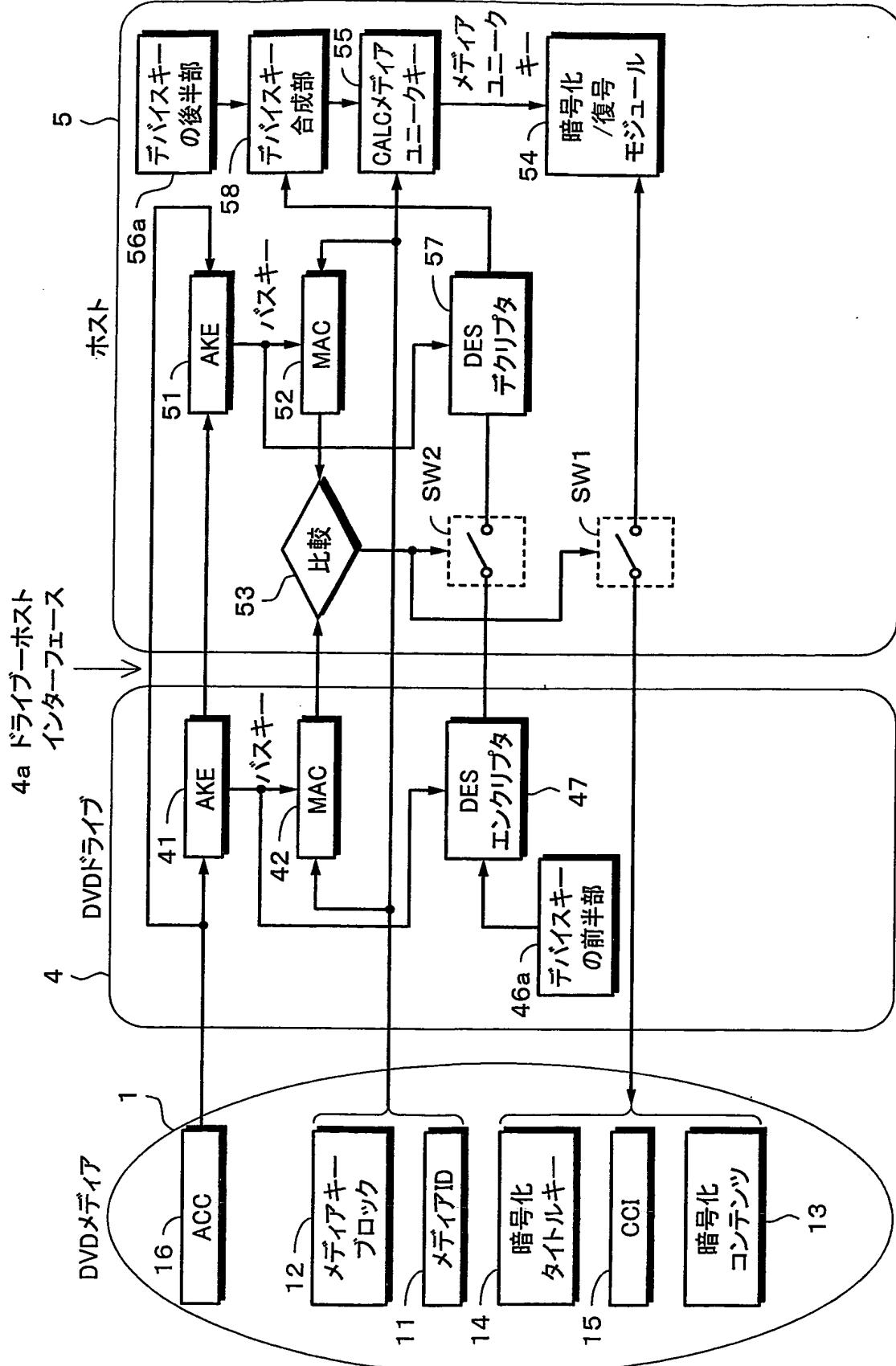
第5図



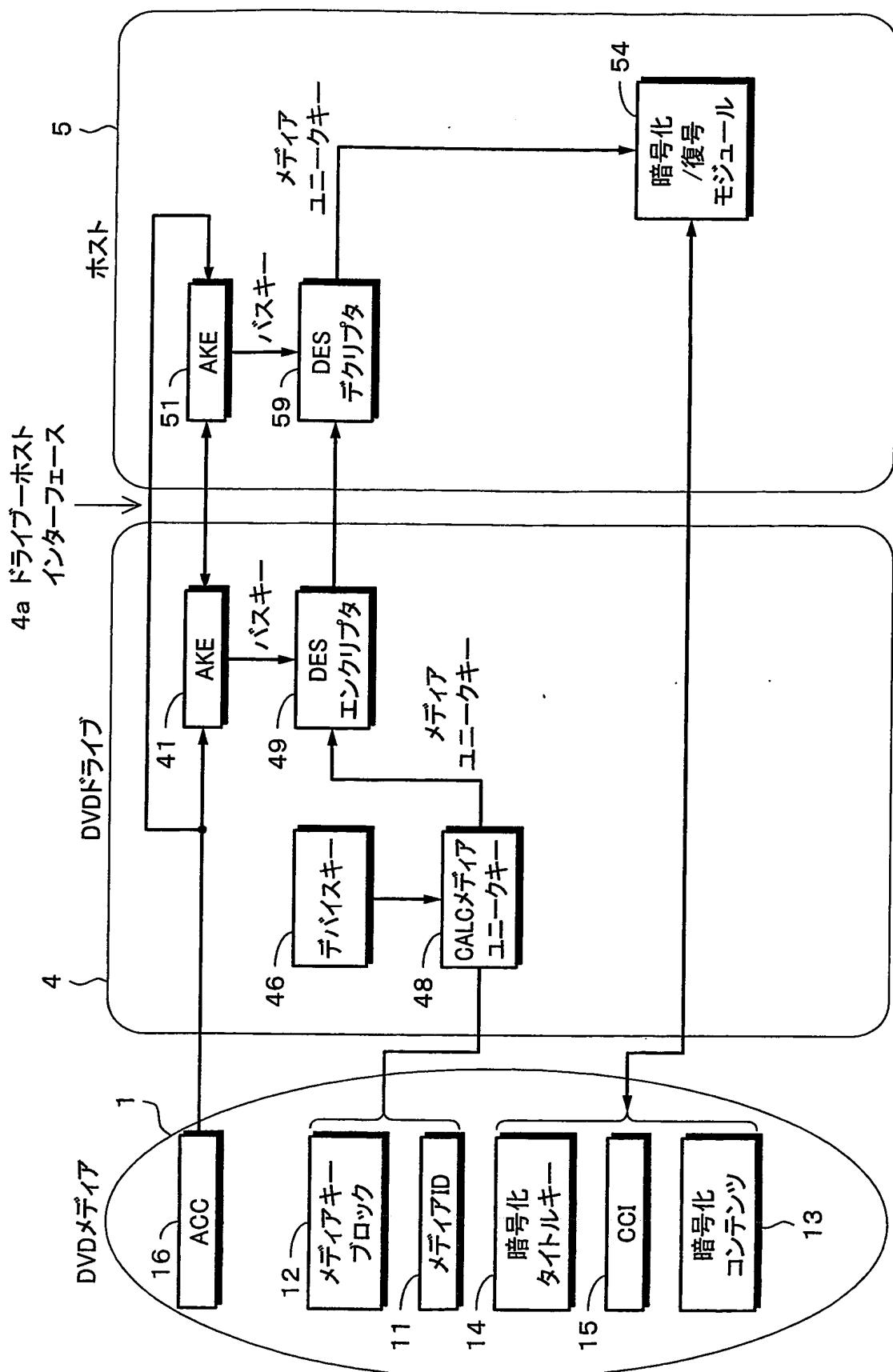
第6図



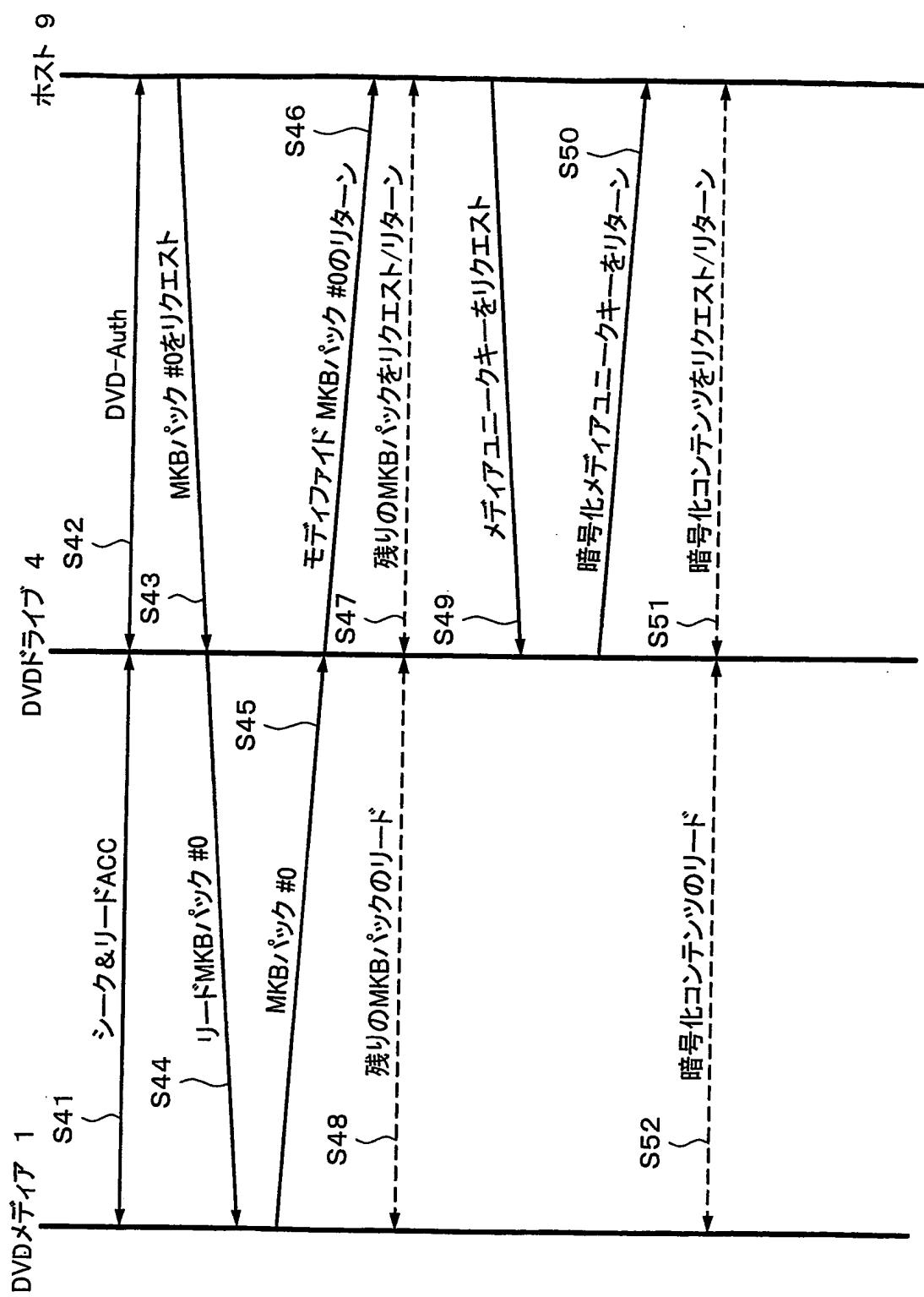
第7図



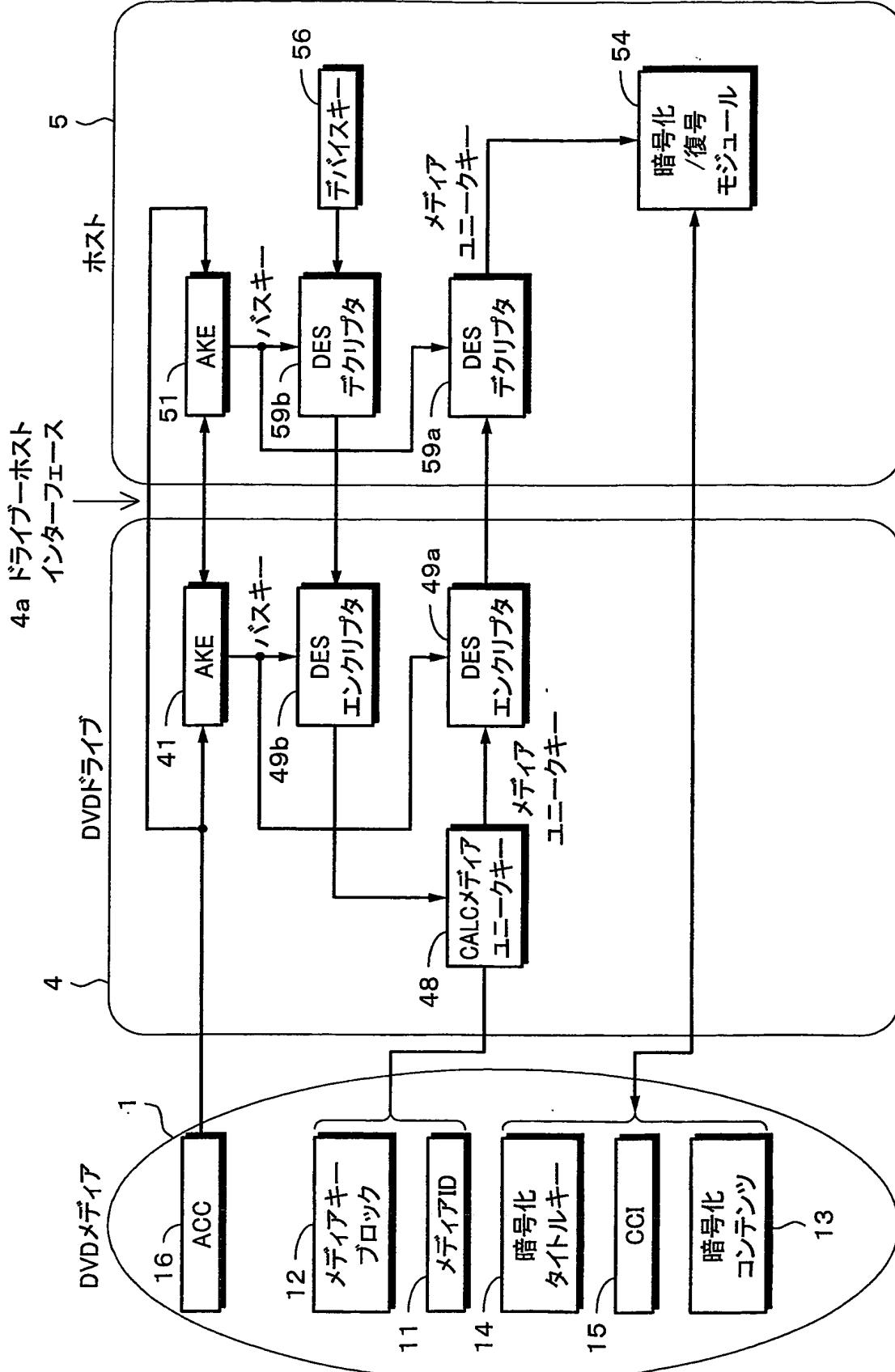
第8図



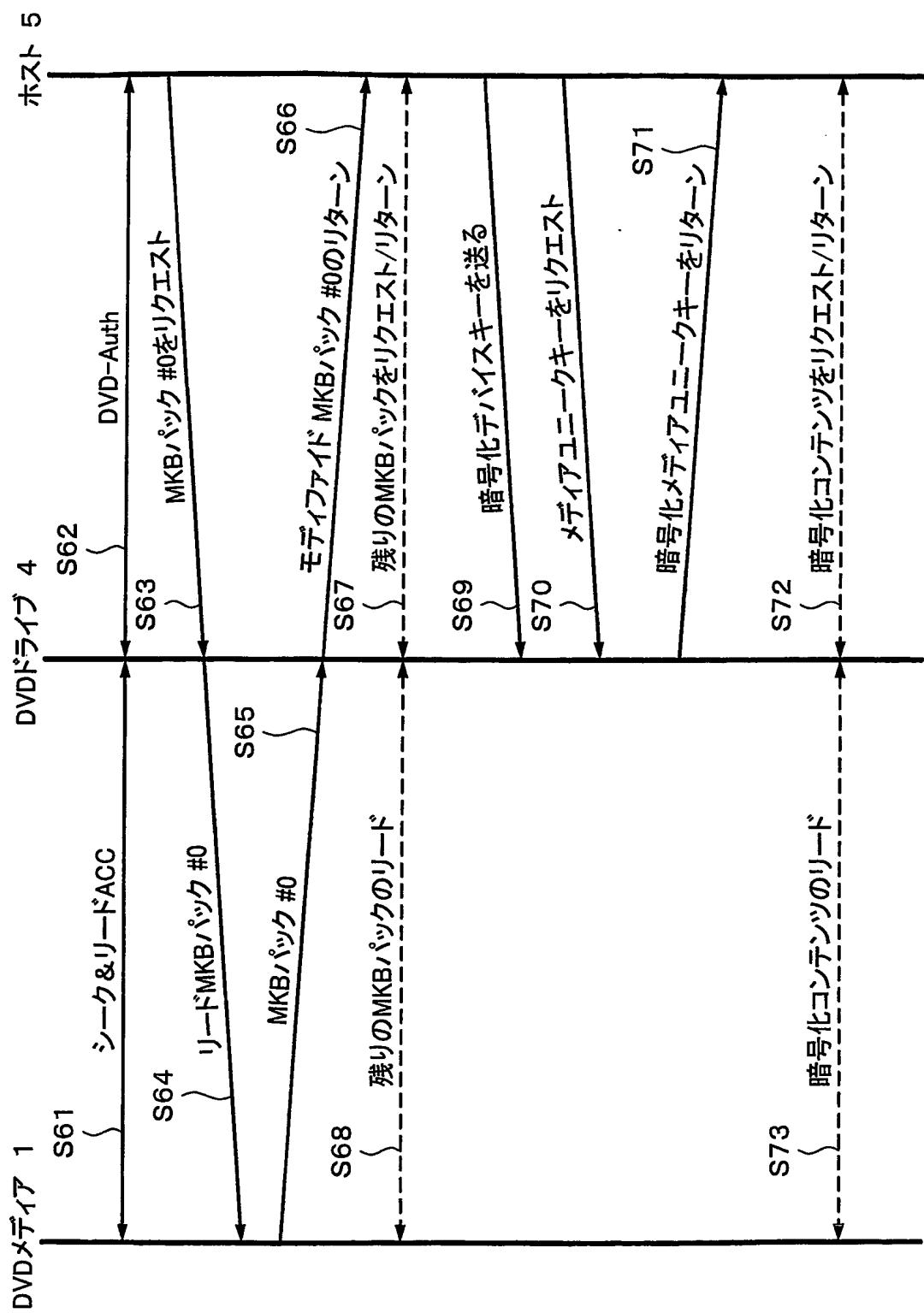
第9図



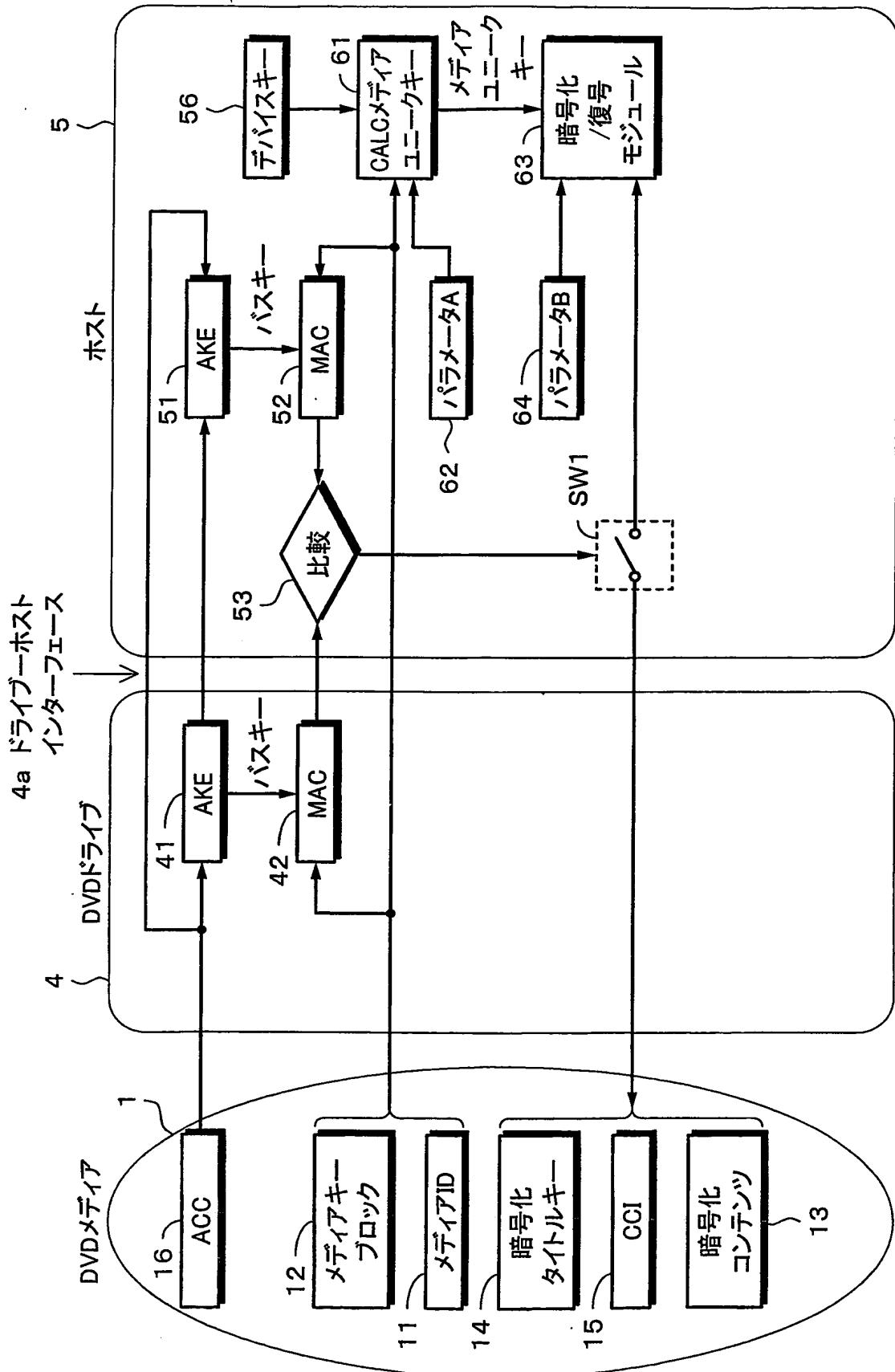
第10図



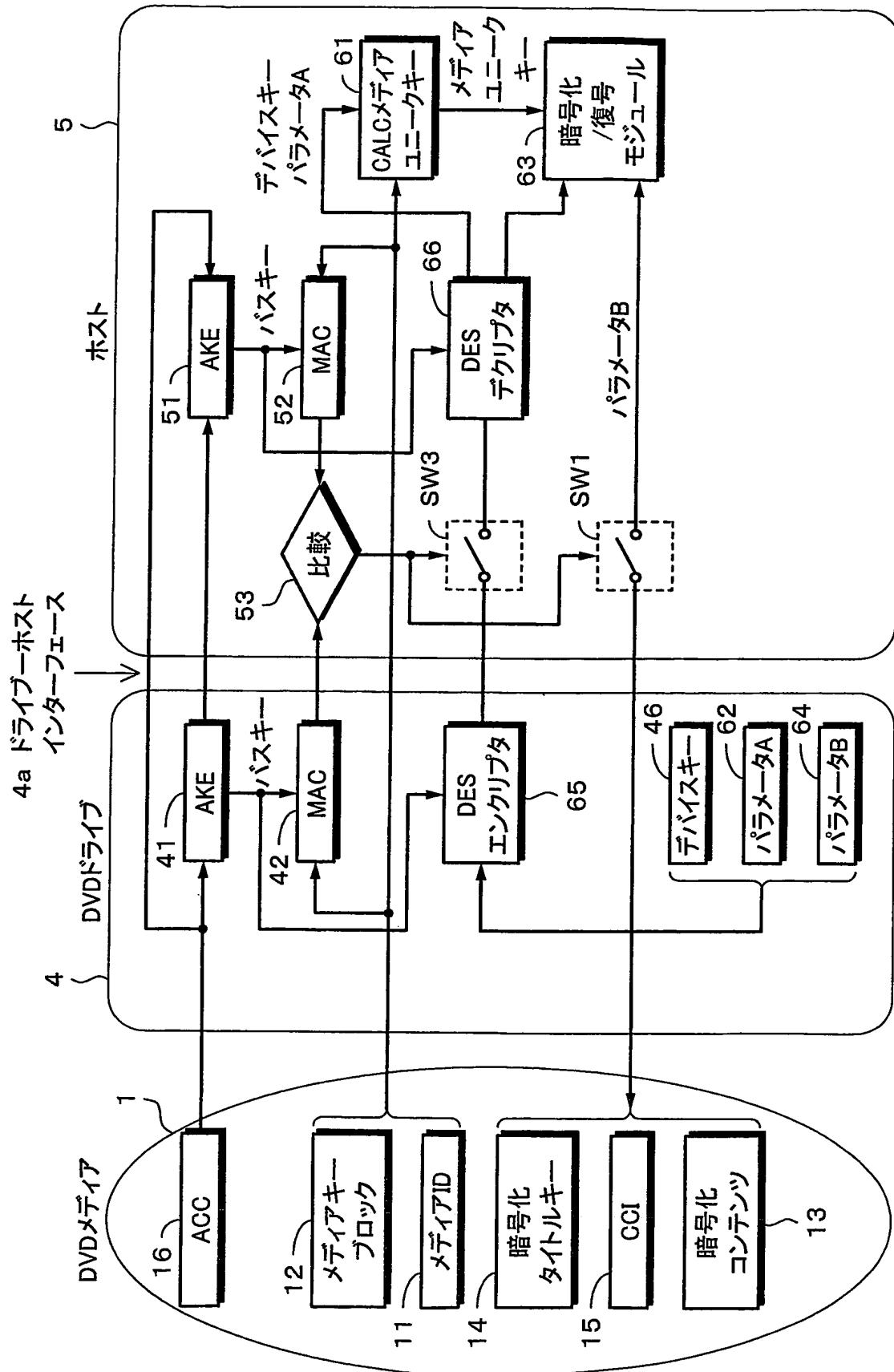
第11図



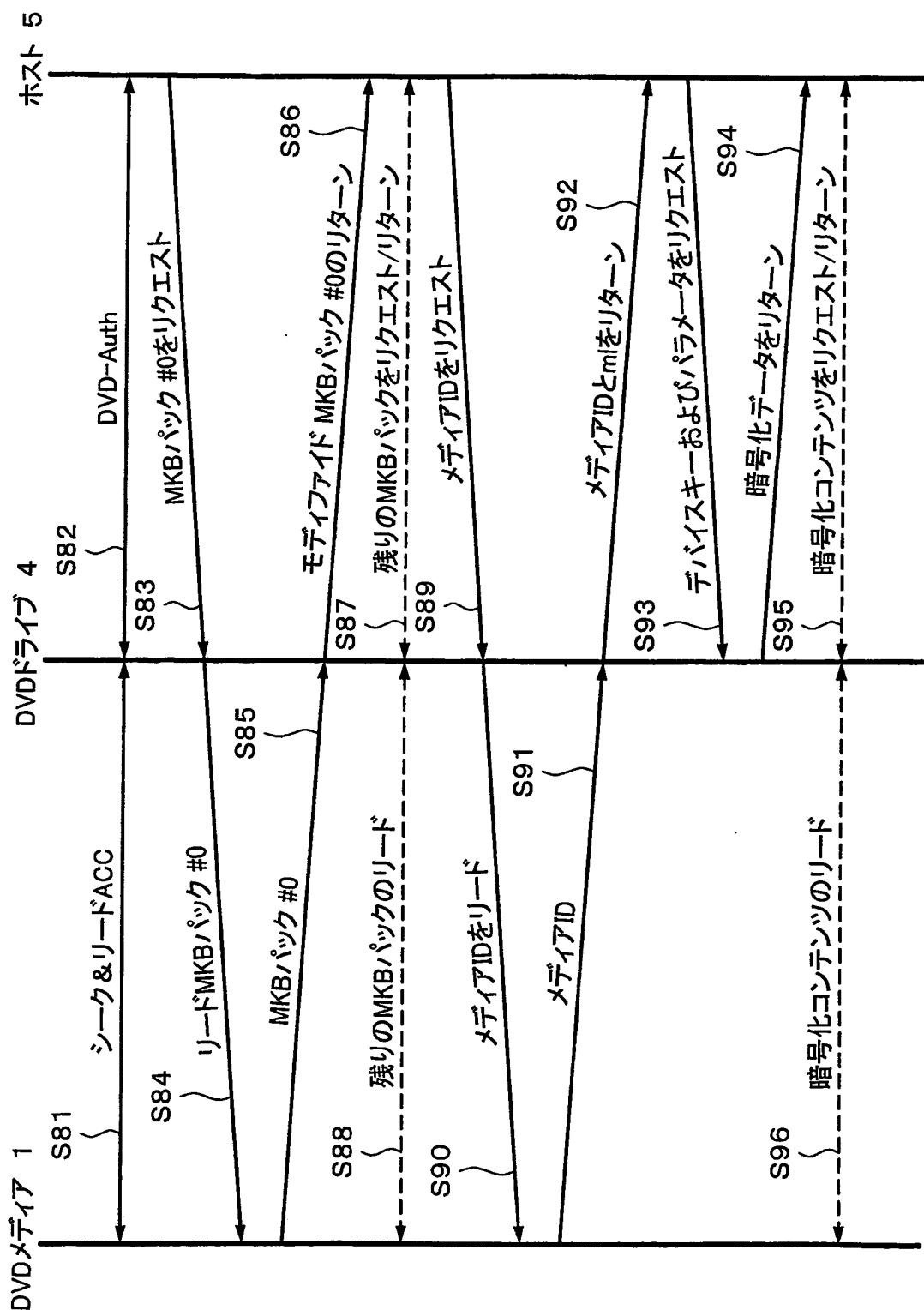
第12回



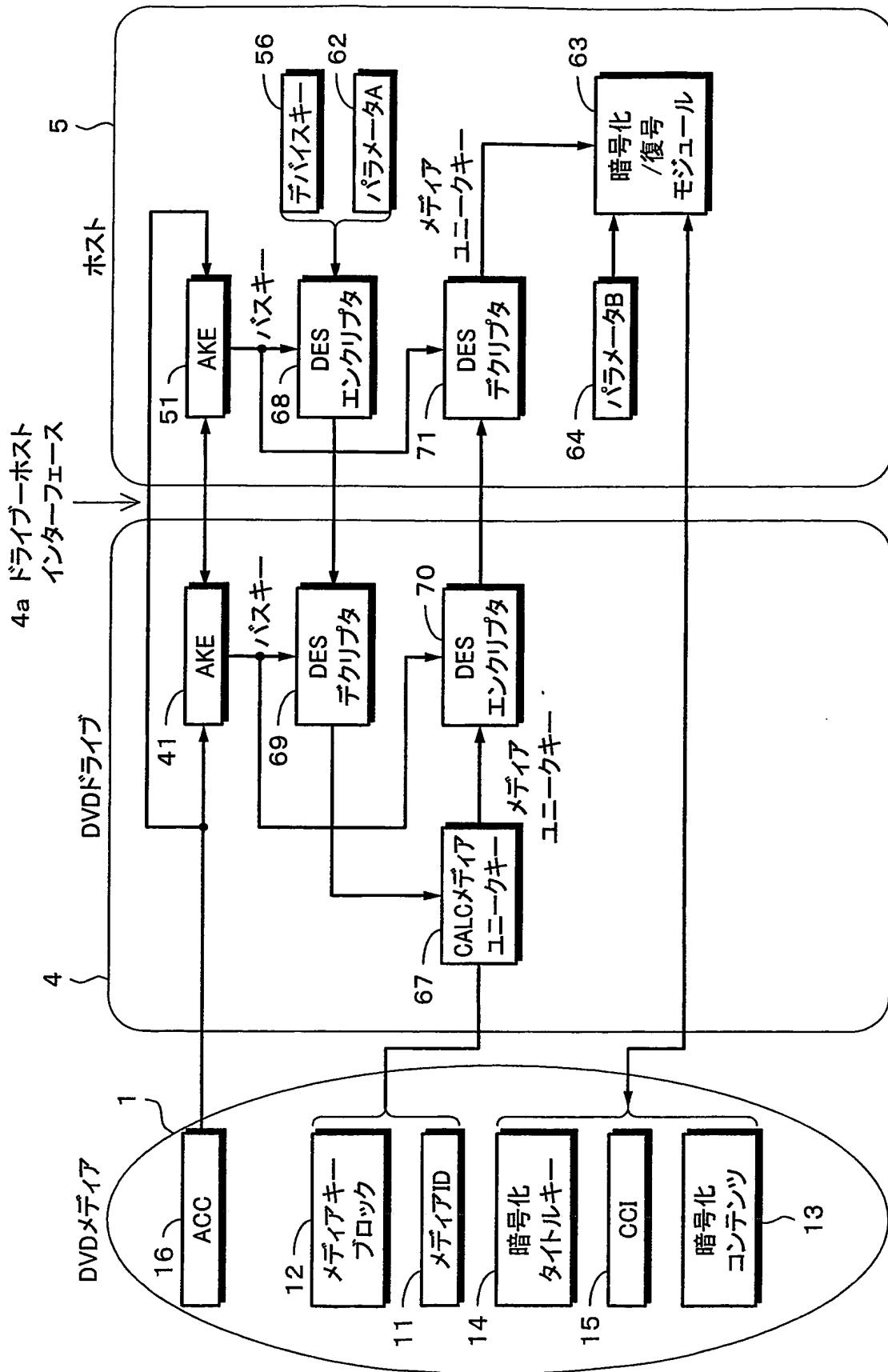
第13図



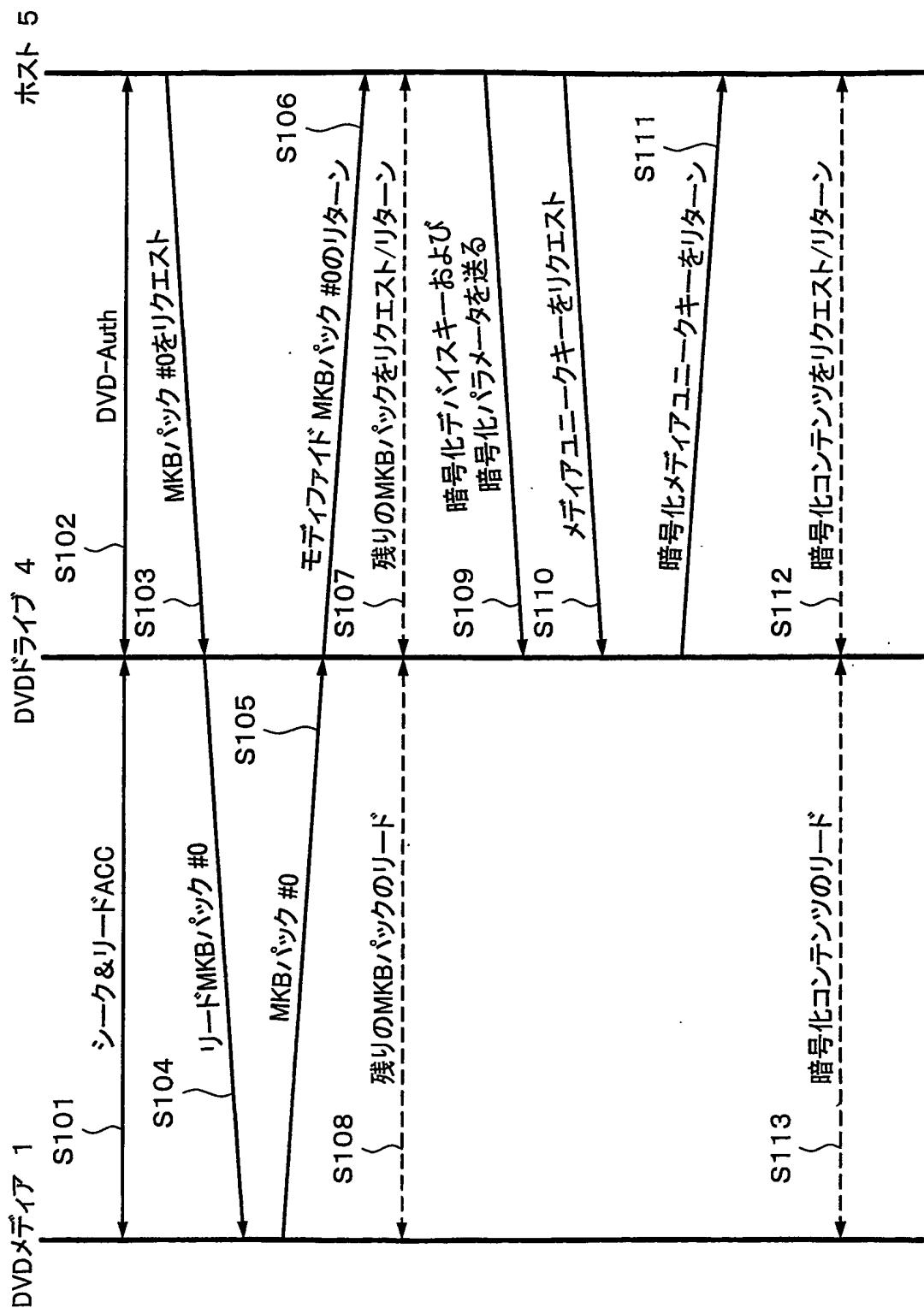
第14図



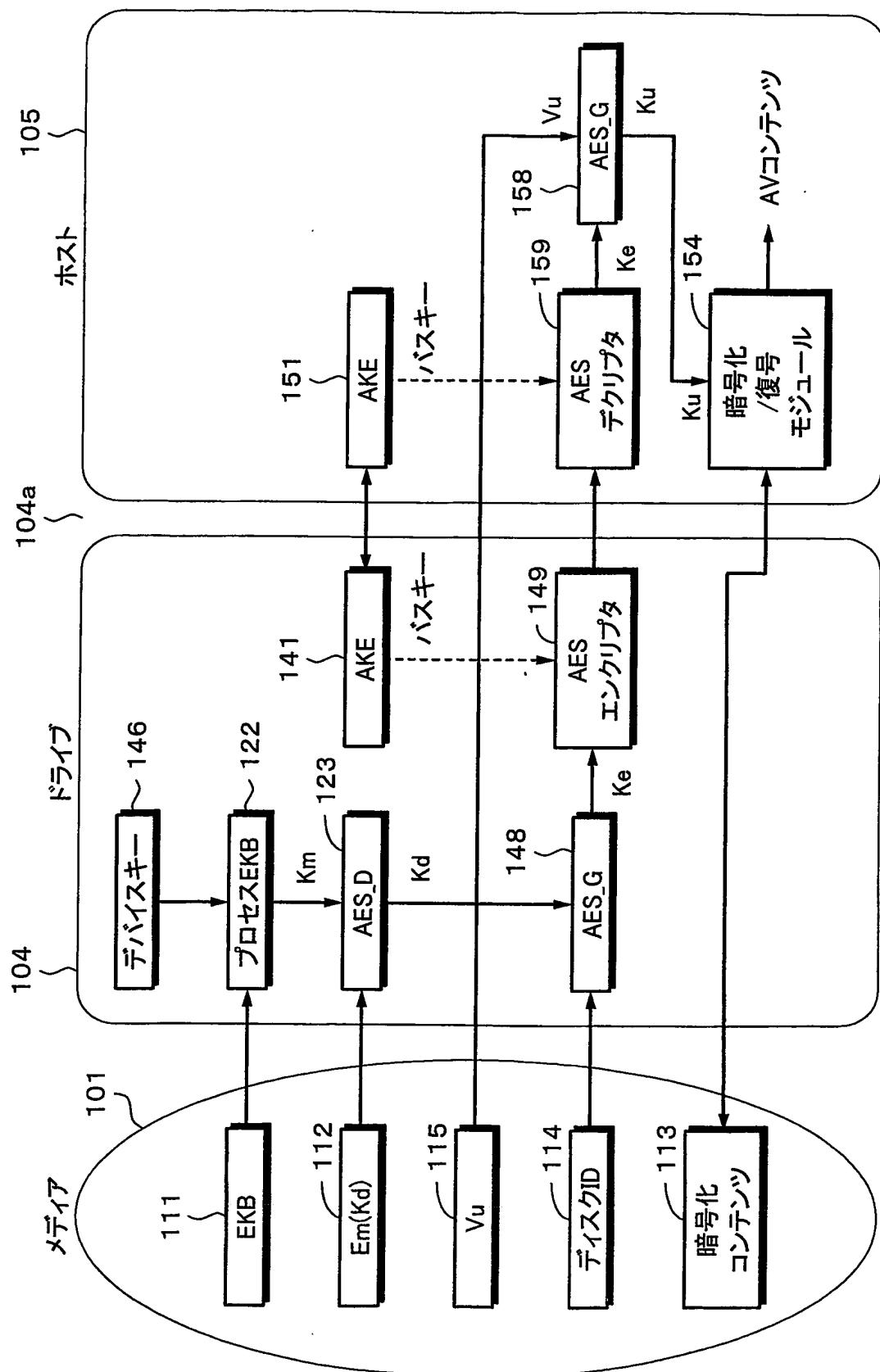
第15図



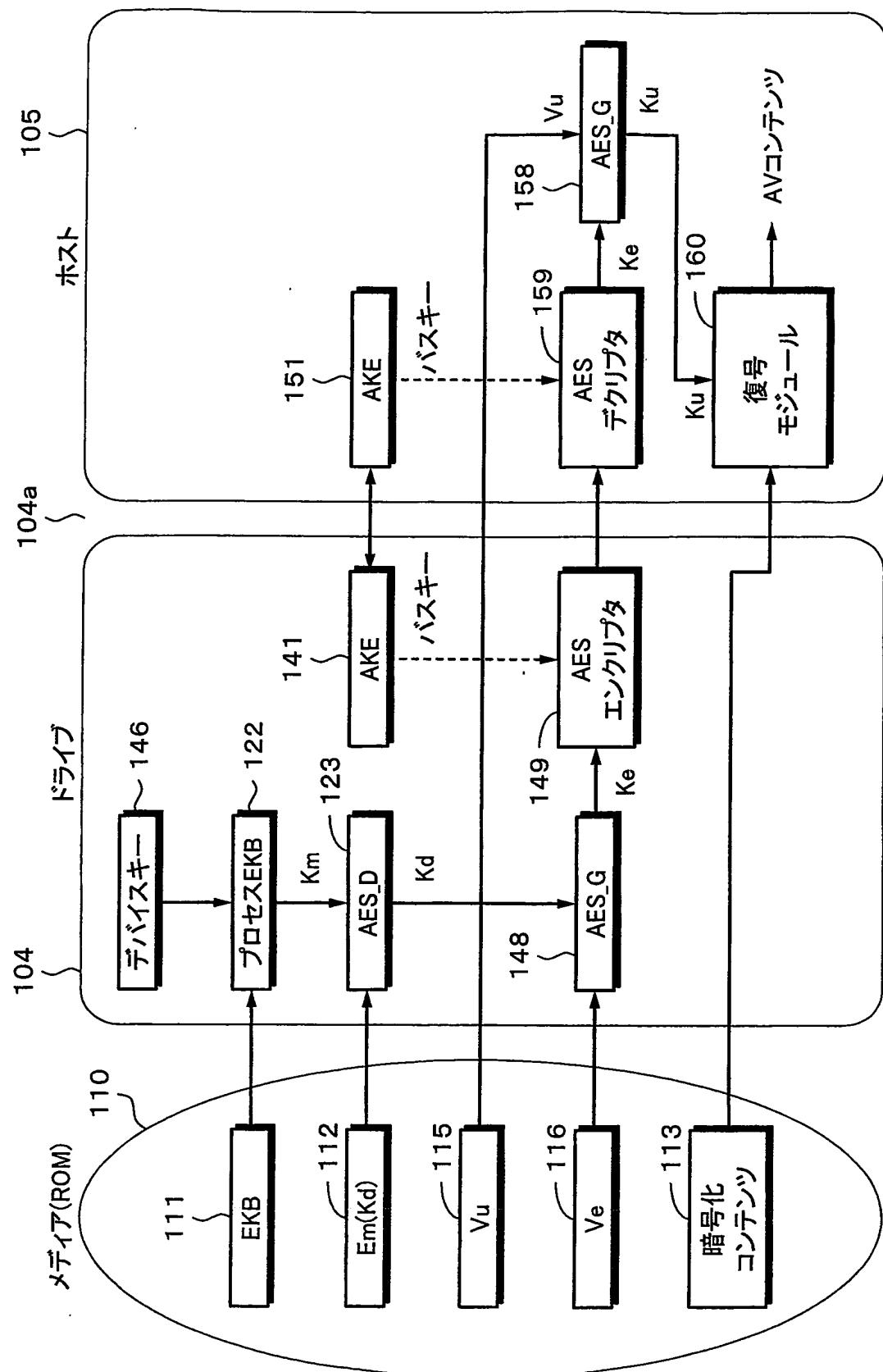
第16図



第一七四



第18回



符号の説明

ST1 MAC計算値が一致？

ST2 スイッチをON

ST3 スイッチをOFF

1 DVDメディア 2 レコーダ 3 プレーヤ

4 DVDドライブ 4a インターフェース 5 ホスト

11 メディアID 12 メディアキーブロック (MKB)

13 暗号化コンテンツ 42, 52 MAC演算ブロック

46 デバイスキーキー 46a デバイスキーキーの前半部

47 DESエンクリプタ

48 メディアユニークキー演算ブロック

49, 49a DESエンクリプタ

49b DESデクリプタ 53 MACを比較する比較

54 暗号化／復号モジュール

55 メディアユニークキー演算ブロック

56a デバイスキーキーの後半部 57 DESデクリプタ

58 デバイスキーキー合成部 59, 59a DESデクリプタ

61 メディアユニークキー演算ブロック

62 パラメータA 63 暗号化／復号モジュール

64 パラメータB 65 DESエンクリプタ

66 DESデクリプタ

101 メディア 104 ドライブ 105 ホスト

111 EKB 112 暗号化ディスクキー

113 暗号化コンテンツ 114 ディスクID

115 ユニットキー生成用値 116 エンベディッドキー生成値